Barracuda Networks Technical Documentation

Barracuda NG Firewall

Release and Migration Notes

Version 5.2.3

RECLAIM YOUR NETWORK™

Copyright Notice

Copyright 2004-2012, Barracuda Networks
www.barracuda.com
v5.2.3-120221-02-0221
All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice.

Trademarks

Barracuda NG Firewall is a trademark of Barracuda Networks. All other brand and product names mentioned in this document are registered trademarks or trademarks of their respective holders.

Content

General 6

GPL Compliance Statement 6

Known Issues 7

Updates with Firmware 5.2.3 7

Update Matrix 7

Software Modules and Components Affected by Minor Release 5.2.3 8

What´s New with Barracuda NG Firewall 5.2.3? 9

Highlights 9

IPFIX Support 9

Support for XEN Virtualization 9

GUI Simplification and Renaming 10

Activation and Licensing Related Features 10

Pool Licensing 10

License Expiration Behavior 10

Admin and Control Functions 11

Control > Box > Network Configuration Activation 11

Control > Network Now Displays Additional DHCP Information 11

Simplified Administrator Configuration 12

Network and Traffic Shaping 12

Simplification and Renaming of the Network Configuration 12

New Auto-Route Creation 13

Remote Management Tunnel for All Product Types 15

Custom Network Objects Based on External Sources 16

Changed Semantics for Traffic Shaping 16

Firewall, IPS and Application Detection 17

Generall Firewall Configuration 17

General Firewall: Kernel Ruleset Renamed to Rule Matching Policy 18

General Firewall: Operational 18

General Firewall: Maximum Number of Allowed SIP Sessions 19

Firewall Rule Editor Usability Improvements 20

IPS Default Read Only 21

IPS Interface Improvements 22

QoS and Application Detection 22

Web Proxy 23
Update of Underlying Squid Engine to Support Multiple Cores 23
Dedicated DNS Settings for Proxy 24
Proxy ACL Based on Geo Location Time Zone 25
Virus Scanner (Malware Protection) 25
Simplification of Virus Scanner Configuration 25
VPN and WAN Optimization 26
XAUTH Authentication Support 26
One Time Password (OTP) Support for SSL VPN 26
Simplification of VPN Service Configuration 26
Advertise Remote Network Routes Via OSPF/RIP for IPSEC Site-to-Site 27
VPN Access Enforcement Based on Windows Security Center Settings 27
WAN Optimization 28
WAN Optimization in GTI 28
WAN Optimization: Warning Display for Encrypted Ports 29
WAN Optimization and VPN Tunnel Compression Compatibility 29
WAN Optimization : Show Compression Statistics 30
SSL VPN & NAC: Centrally Managed Password for NAC Deactivation 30
Control Center Related Changes 31
RCS Now Logs Changes Made Via GTI Editor Changes 31
Additional Migration Cluster 31
Other 31
Box Properties Configuration Node 31
Password Strength Meter 31
Updated Password Entry Configuration Object 32
SSH Proxy: 33
Simplification and Renaming of Server Configuration 34
Create PAR Files for Single Units on NG Control Center 34
New Semantics 34

What´s New with Barracuda NG Network Access Client 2.0 SP6? 38

User Client Shutdown Password Centrally Manageable 38
Immediate Health Validation on Demand 38
Automatically Enable Quarantine, Receive Power Setting Notifications and Suppress Activity in Suspend Mode 38
Automatic VPN Termination on Unhealthy or Untrusted Client 38
Default Quarantine Ruleset on Personal Firewall Start 39
VPN Probing Uses Windows Settings to Connect 39
Regrouped Advanced Profile Settings 39
VPN Profile Wizard X.509 Configuration Extended 39
VPN DNS Domain Name Conflict Prevention 39
Changed Multiple X.509 Certificates Handling 40
Access Control Server Certificate Check 40
Health Agent Monitors Certification Authorities 40
Trust Chain Manager 40
New Health Agent Registry Entry 41
VPN Profile Creation from a *.VPN File 41
Aggregate Health State for Windows Security Provider 41
Registry Setting to Prevent OPSWAT Initialization 42
Decreased Default MTU Size 42

Nagle's Algorithm Enabled for VPN Sockets 42
Registry Flag to Prevent Automatic X.509 Serial Number Updates 43
Updated OPSWAT Libraries 43

Bugfixes Included with Barracuda NG Firewall 5.2.3 44

Barracuda NG Admin 44
Barracuda NG Installer 44
Barracuda NG Network Access Client 2.0 SP6 45
Barracuda NG Firewall 45

Supported Hardware 49

Determine Your Update Scenario 50

Combining NG Control Center 5.2.x with 5.0.x and/or 4.2.x Units 52
Solving Update and Installation Failures 52

Updating Unmanaged Units or NG Control Centers 53

Updating Units or NG Control Centers using SSH 53

Updating HA-Synced Units or HA-Synced NG Control Centers 54

Updating NG Control Center Managed Units 56

Updating Standard Hardware from 4.2.x to 5.2.3 58

General 58
Updating Procedure 58

General

Warning

Read this document **before** updating your system

Caution

If you are going to update from **release version 4.2** to Barracuda NG Firewall 5.2.3 via firmware version 5.0 (no direct update is possible!), Barracuda Networks strongly recommends to study the **Barracuda NG Firewall 5.0 Migration Instructions** and also the **Barracuda NG Firewall 5.2 Migration Instructions** available for download at **https://login.barracudanetworks.com**, as, under certain circumstances, no countermanding is possible once the updating process was initiated.
There you will also find in-depth information on new features and changes in terminology that have been introduced with release version 5.0.

Caution

Starting with Barracuda NG Firewall 4.2.13, OVA images for VMWare were made available. OVA images based on minor release 4.2.13 have a bug which might lead to loss of the current network configuration when updating to Barracuda NG Firewall minor release version 5.2.3 via major release version 5.0.
Please make sure to configure your network settings **before updating** virtual appliances based on 4.2.13 OVA images using Barracuda NG Admin at least once. Also, a network activation is required.
This issue does not apply to fresh installations based on 5.2.3 OVA images.

Note

Prior to firmware release version 5.2.3 it was for compatibility reasons possible to establish a client-to-site VPN connection by only using any VPN client even though Exclusive Network Access (ENA) was configured on the Barracuda NG Firewall.

With 5.2.3, it is now implicitly necessary to have the NG Personal Firewall including the packet filter SPAC installed on the client, otherwise a connection to the VPN server will be prevented.

Note

One time password authentication with Verisign's Unified Authentication Tokens will only work if the new ***OTP preserves State*** configuration parameter in the ***RADIUS*** configuration of Barracuda NG Firewall is properly set.

This parameter is only visible in ***Advanced*** mode.

Note

The Barracuda NG Firewall may reboot after installation. If not, Barracuda Networks recommends performing a manual reboot.

GPL Compliance Statement

This product is in part Linux based and contains both Barracuda Networks proprietary software components and open source components in modified and unmodified form. A certain number of the included open source components underlie the GPL or LGPL or other similar license conditions that require the respective modified or unmodified source code to be made freely available to the general public, this source code is available on http://source.barracuda.com.
Please also refer to the chapter ***Warranty and Software License Agreement*** of the Barracuda NG Firewall 5.2.3 Administrator's Guide documentation located in the documentation section on www.barracuda.com and on each accompanying USB thumb drive.

Known Issues

Note

Advice about known issues is available through **https://login.barracudanetworks.com/support/knownissue** or through the Barracuda Networks Technical Support.

Updates with Firmware 5.2.3

Update Matrix

Table 1–1 Update matrix - supported and not supported update cases

Current Version	Target Version									
	5.0	**5.0.1**	**5.0.2**	**5.0.3**	**5.0.4**	**5.0.5**	**5.2.0**	**5.2.1**	**5.2.2**	**5.2.3**
4.2.10 and earlier	-	-	-	-	-	-	-	-	-	-
4.2.11	✓	✓	✓	✓	✓	✓	-	-	-	-
4.2.13	✓	✓	✓	✓	✓	✓	-	-	-	-
4.2.14	✓	✓	✓	✓	✓	✓	-	-	-	-
4.2.15	✓	✓	✓	✓	✓	✓	-	-	-	-
4.2.16	✓	✓	✓	✓	✓	✓	-	-	-	-
4.2.17	✓	✓	✓	✓	-	✓	-	-	-	-
4.2.18	✓	✓	✓	✓	✓	✓	-	-	-	-
5.0	-	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.0.1	-	-	✓	✓	✓	✓	✓	✓	✓	✓
5.0.2	-	-	-	✓	✓	✓	✓	✓	✓	✓
5.0.3	-	-	-	-	✓	✓	✓	✓	✓	✓
5.0.4	-	-	-	-	-	-	-	-	✓	✓
5.0.5	-	-	-	-	-	-	-	-	-	✓
5.2.0	-	-	-	-	-	-	-	✓	✓	✓
5.2.1	-	-	-	-	-	-	-	-	✓	✓
5.2.2	-	-	-	-	-	-	-	-	-	✓

Software Modules and Components Affected by Minor Release 5.2.3

Table 1–2 Affected Software Modules and Components

		Affected by Minor Release		
		5.2.1	5.2.2	5.2.3
Software Modules	Firewall	✓	✓	✓
	VPN Service	✓	✓	✓
	Access Control Service	-	✓	✓
	HTTP Proxy	✓	✓	✓
	Secure Web Proxy	-	✓	✓
	URL Filter	-	✓	-
	Mail Gateway	✓	-	✓
	Spam Filter	-	-	-
	Virus Scanner	-	✓	✓
	DHCP Service	✓	✓	-
	DHCP Relay	-	-	-
	DNS	-	✓	-
	FW Audit Log Service	-	-	-
	FTP Gateway	-	✓	-
	OSPF/RIP Service	-	-	-
	SNMP Service	✓	-	✓
	SSH Proxy	-	-	-
	Authentication	✓	-	✓
Other	Barracuda OS	✓	✓	✓
	NG Control Center	✓	✓	✓
	Network	✓	✓	✓
	NG Admin	✓	✓	✓
	NG Install	✓	✓	✓
	NG Network Access Client	-	-	✓
	NG VPN Client 3.0 for MacOS	-	-	-

What´s New with Barracuda NG Firewall 5.2.3?

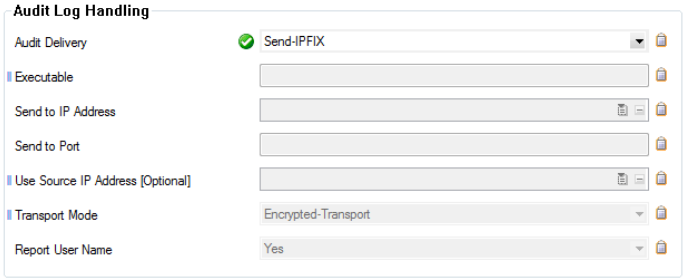
Firmware release version 5.2.3 of Barracuda NG Firewall comes with a variety of new features and improvements that are described below.

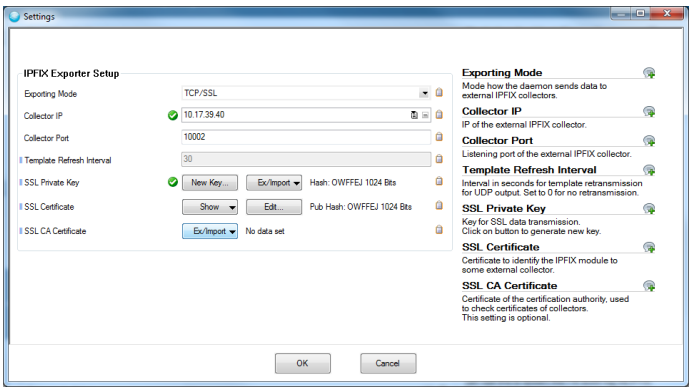
For an exact description of the numerous changes in GUI semantics **see New Semantics, Page 34.**

Highlights

IPFIX Support

Starting with firmware release version 5.2.3, Barracuda NG Firewall introduces IPFIX streaming support (Internet Protocol Flow Information Export RFC3917) in order to stream all firewall audit logs and HTTP proxy access cache logs to an IPFIX / NetFlow collector.





Support for XEN Virtualization

Starting with firmware release version 5.2.3, Barracuda NG Firewall XEN compatible images will be provided for basic (plain) XEN images (`.zip` in the download section covering paravirtualization and full virtualization) and Citrix compatible paravirtualization (`.pv.xva`) and fully virtualized (`.hvm.xva`) images.

GUI Simplification and Renaming

Huge portions of the interface were reworked to be more intuitive to use, faster to set up a single Barracuda NG Firewall unit and conforming to industry naming standards.

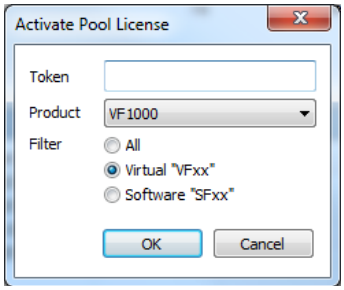
Activation and Licensing Related Features

Pool Licensing

Starting with firmware release version 5.2.3, Barracuda NG Firewall and Barracuda NG Control Center support floating pool licensing for VFxxx and SFxxx licenses.

To activate a pool license on a Barracuda NG Control Center have your activation code ready and navigate to ***Control -> Barracuda Activation***, then select ***Import Pool License***.

The figure below shows how to enter a License Token for VFxxx units:



Note

Pool licenses always need to be activated on Barracuda NG Control Center units (virtual or hardware).

License Expiration Behavior

Starting with firmware release version 5.2.3, the license expiration behavior of single unmanaged units has changed. Upon expiration of the basic unit license, the services contained within the BASE license are no longer shut down but keep on running instead.

Note

Content Security and SSL VPN and NAC services will be shut down immediately, therefore e.g. the Virus Scanner will no longer be available. Also, pattern updates will in this case no longer be applied to content security options like malware protection and IPS.

The configuration of the unit in Barracuda NG Admin is now frozen and no modifications can be done with the following exceptions: Importing a PAR file and entering a new license.

Two standalone units in HA configuration behave as follows: the unit with the expired license will still receive configuration updates from the active unit if the active unit still has a valid license.

License expiration behavior of centrally managed units is not affected by this change. If the license for a centrally managed unit expires, or the license stamp was not renewed by the Barracuda NG Control Center for pool licenses, all services will be shut down and the unit will stop forwarding traffic.

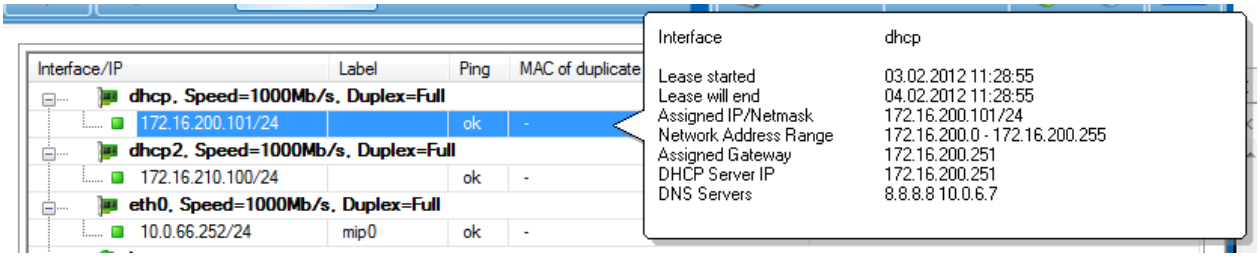
Admin and Control Functions

Control > Box > Network Configuration Activation

Starting with firmware release version 5.2.3, the network activation appearing subsequent to changes in the network configuration is optimized for performance. Especially on low-end Barracuda NG Firewall units like F10 up to F200 the improvement should be noticeable.

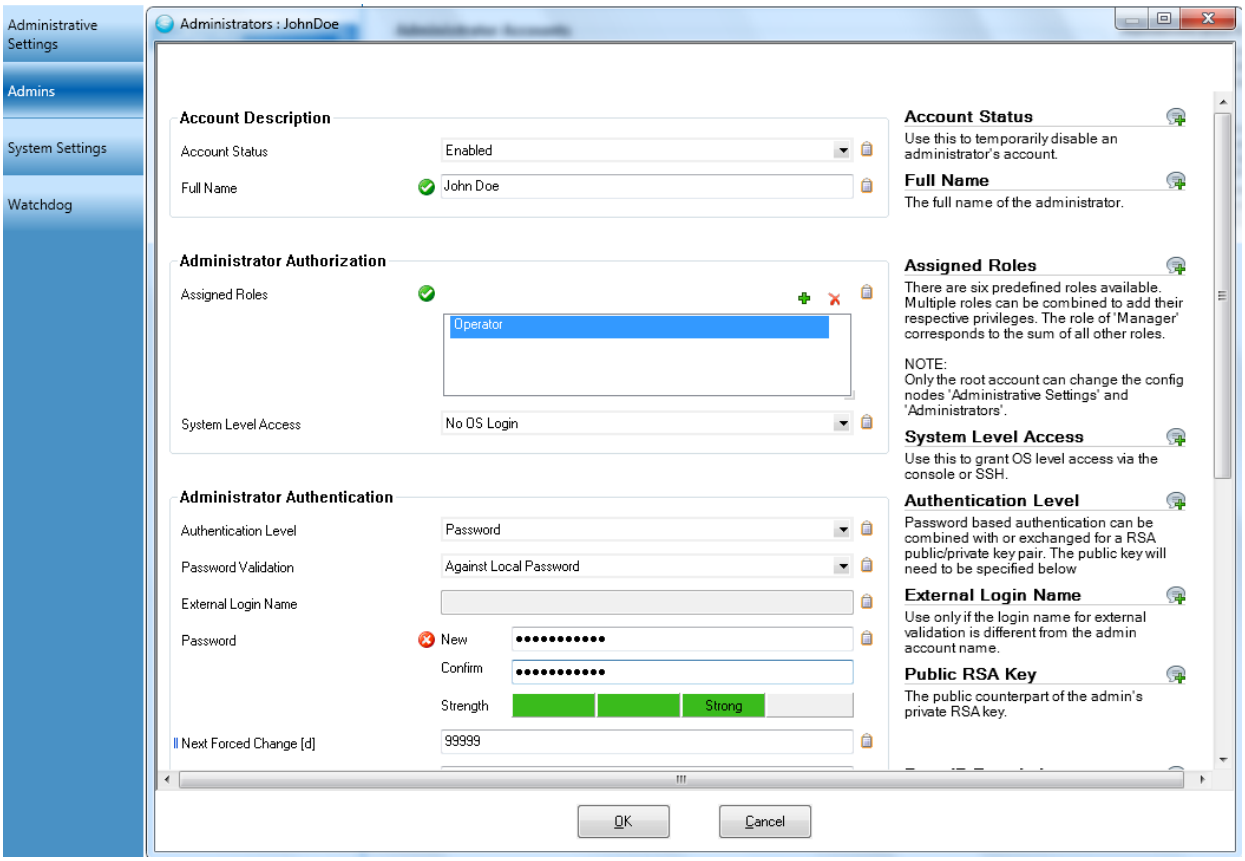
Control > Network Now Displays Additional DHCP Information

Starting with Barracuda NG Admin 5.2.3, hovering the mouse pointer over a DHCP assigned IP address in the ***Network*** view will result in the appearance of a tooltip-like window that contains additional DHCP information.



Simplified Administrator Configuration

With firmware release version 5.2.3, rarely needed settings were moved into the ***Advanced*** view mode. In addition, the help comments on the right side of the user interface were improved in order to enhance the ease of use.


Administrative Settings
Admins
System Settings
Watchdog
Administrators : JohnDoe
Account Description
Account Status
Enabled
Full Name
John Doe
Administrator Authorization
Assigned Roles
Operator
System Level Access
No OS Login
Administrator Authentication
Authentication Level
Password
Password Validation
Against Local Password
External Login Name
Password
New
Confirm
Strength
Strong
Next Forced Change [d]
99999
OK
Cancel
Account Status
Use this to temporarily disable an administrator's account.
Full Name
The full name of the administrator.
Assigned Roles
There are six predefined roles available. Multiple roles can be combined to add their respective privileges. The role of 'Manager' corresponds to the sum of all other roles.
NOTE:
Only the root account can change the config nodes 'Administrative Settings' and 'Administrators'.
System Level Access
Use this to grant OS level access via the console or SSH.
Authentication Level
Password based authentication can be combined with or exchanged for a RSA public/private key pair. The public key will need to be specified below
External Login Name
Use only if the login name for external validation is different from the admin account name.
Public RSA Key
The public counterpart of the admin's private RSA key.

Network and Traffic Shaping

Simplification and Renaming of the Network Configuration

Starting with firmware release version 5.2.3, the network configuration was reworked to be more intuitive in usage and to conform to industry naming standards.

Additionally, the help comments on the right side were clarified and expanded throughout all sub screens of the network configuration.

For the ***Management IP Address*** and the ***Network***, a trust level may now be assigned which is available in the ***Advanced*** settings mode.

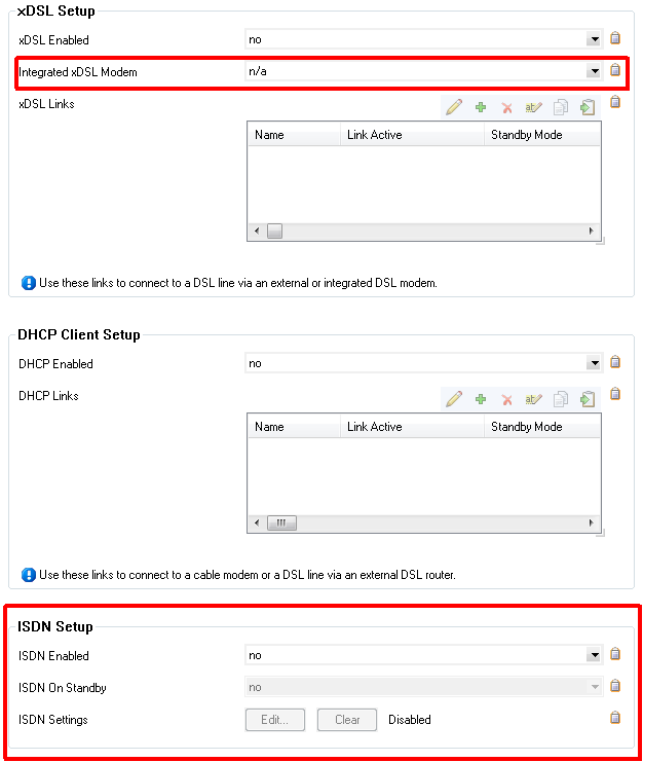
The ***Ethernet Trunks*** configuration was removed from the ***Interfaces*** section. There is now a separate screen named ***Ethernet Bundles*** available within the menu on the left side.

The ***Virtual LAN*** properties and creation screen have been reworked.

Within the ***Routing*** properties and ***Routing Rules*** creation, a new ***Route Origin*** field was added. It is used to indicate the origin of the entry. If created manually, the route displays ***User created*** as its origin. ***Origin Auto created*** denotes routes resulting from settings made by e.g. ***Auto-Route Creation*** (see below). This means the certain settings cannot be edited within this part of the configuration to avoid ambiguity.

The setup for ISDN as well as for the integrated DSL modem was moved to ***Advanced*** view mode.

.

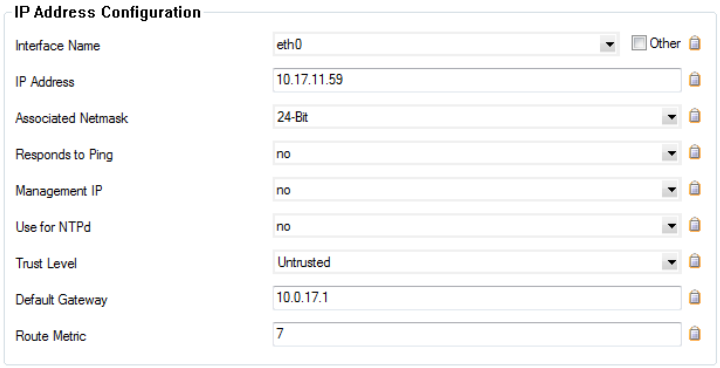


New Auto-Route Creation

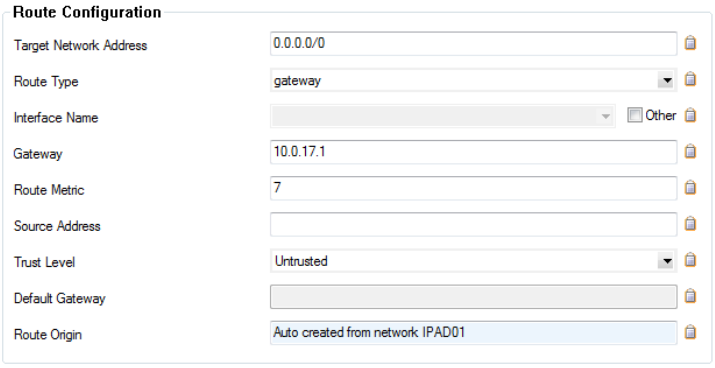
In order to speed up new deployments, the tasks of configuring an IP address and the associated route to the intenet for a unit were automated, so that the routes, and if needed policy routes, are created automagically.

If within ***IP Configuration > Additional Local IPs*** a ***Default Gateway*** is specified, then a matching next-hop route entry will automatically be created during activation. If during the additional ***local IP*** configuration the ***Trust Level*** is set to ***Untrusted***, the next activation process will also automatically create a source-based routing entry (a.k.a policy route).

The figure below shows the updated IP address configuration dialog with ***Default Gateway*** and ***Trust Level***:

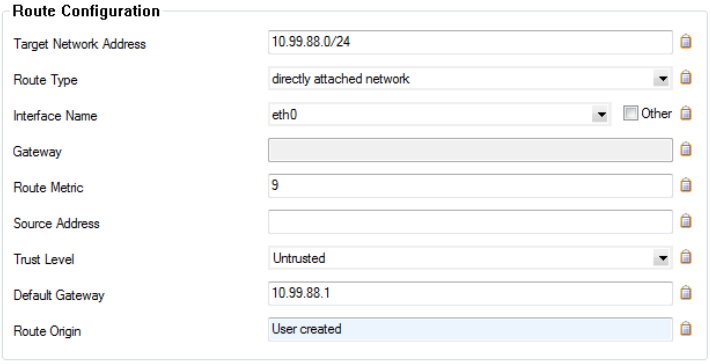


The figure below shows an auto-created route:

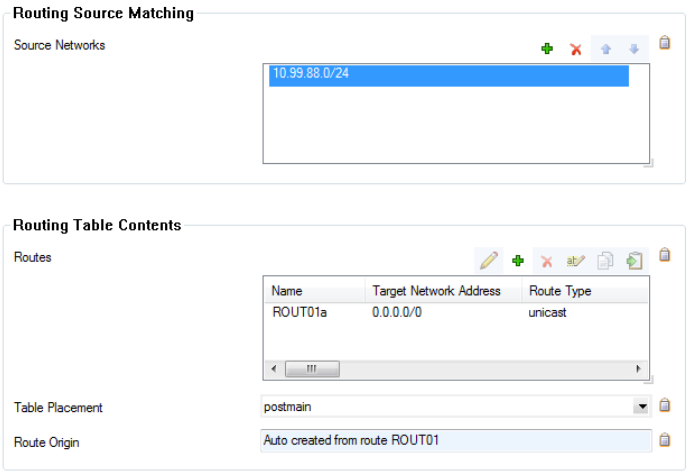


If in the ***Routing*** interface a directly attached network is specified with ***Trust Level*** set to ***Untrusted,*** a matching source-based routing entry (a.k.a policy route) will automatically be created during activation.

The figure below shows a new directly attached network with a ***Trust Level*** of ***Untrusted***:



The figure below shows an auto-created source-based routing entry for the directly attached network:

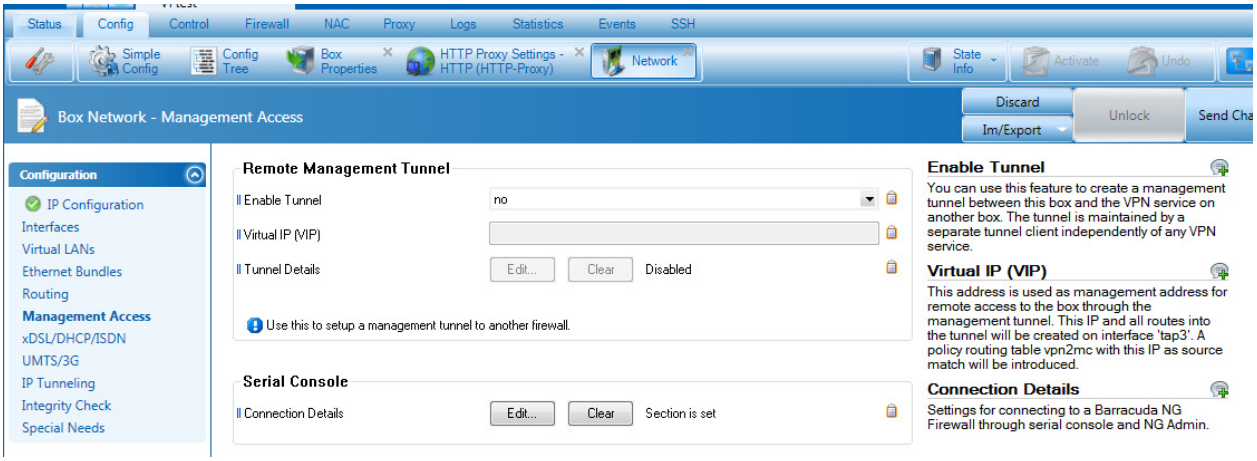


Remote Management Tunnel for All Product Types

Starting with firmware release version 5.2.3, all hardware and license types of Barracuda NG Firewall will provide a way to configure a VPN management tunnel to a remote Barracuda NG Firewall unit. This can be set up within the ***Management Access*** screen of the ***Box Network*** configuration node in ***Advanced*** view mode. The remote management tunnel may be used to conveniently administer a small number of Barracuda NG Firewall units by giving the administrator direct access with just the Barracuda NG Admin application without the need for connecting remotely to the unit. Formerly, this feature was only available for certain appliance types.

Related Docs

See the **Barracuda NG Firewall 5.2.3 Administrator's Guide** for in-depth information on this feature. This document is downloadable through **http://barracuda.com/doc**.



Custom Network Objects Based on External Sources

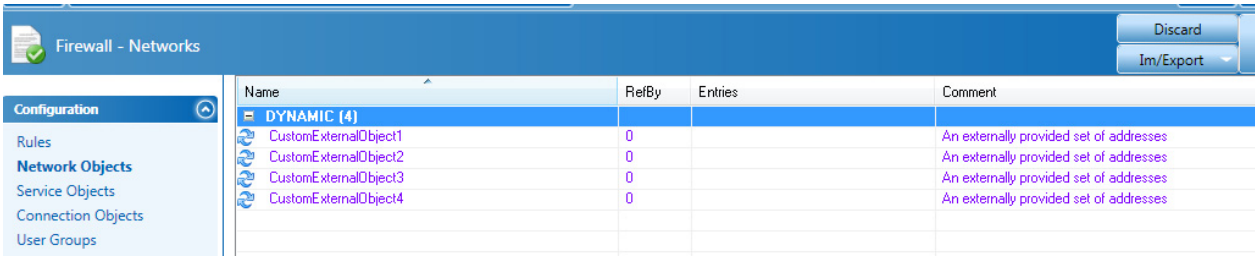
Starting with release version 5.2.3, the firmware provides four custom dynamic network objects to be filled by external sources. This allows e.g. to create firewall rules that block traffic to a list of known botnet members while this list is maintained by a third party.

Related Docs

See the **Barracuda NG Firewall 5.2.3 Administrator's Guide** for in-depth information on this feature. This document is downloadable through **http://barracuda.com/doc**.

Note

This feature has already previously been provided as a hotfix to firmware version 5.2.2.



With firmware release version 5.2.3, certain improvements over the initially provided custom external input function were implemented.

With 5.2.2, this function (`/opt/CustomExternalAddressImport`) could only handle a hard coded maximum of 10,000 addresses. Address content in excess of this limit were not processed. This limit is now configurable via a new option switch, `-l`. If the option is not used, then the default maximum of 10,000 entries applies. The absolute maximum to be supplied using this option switch is 500,000 entries which roughly translates to a RAM usage of 10 megabytes. The input data parsing was changed to be more robust. All non-IPv4 address related characters are not just trimmed from the input data file but replaced by whitespace. This means that e.g. `1.1.1.1;2.2.2.2;3.3.3.3` is now also a legitimate input format. Previously processing the input would have concatenated the addresses into one blob as the semicolon would just have been trimmed.

```
./CustomExternalAddrImport: illegal option -- f
Usage: CustomExternalAddrImport OPTIONS
OPTIONS:
 -l <1-500000>   ... maximum number of allowed address entries
 -h              ... do HA syncc
 -o <1-4>        ... mandatory index of network object
 -i /var/phion/home/<admin>/<filename>     ... mandatory input data file
```

Changed Semantics for Traffic Shaping

Firmware release version 5.2.3 introduces a changed Traffic Shaping nomenclature. Shaping Connector is now called ***QoS Band***, Virtual Shaping Tree is now named ***QoS Profile***. Former Templates were renamed to ***Predefined Profiles***, Basic Scheme to ***Basic Profile*** in the Traffic Shaping config and the operational GUI. Within the firewall rule set, Forward and Reverse shaping were renamed to ***QoS Band***

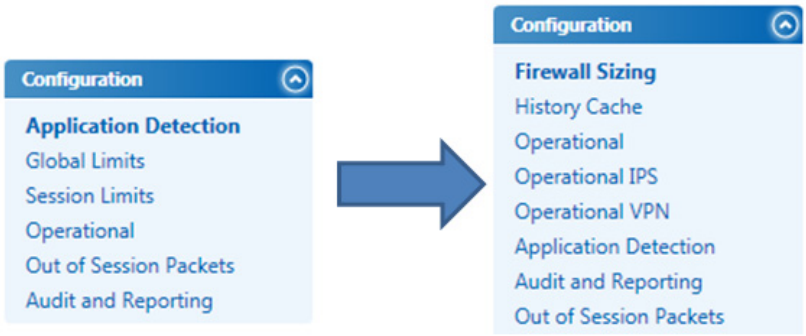
(Fwd) and ***QoS Band (Reply)***.

Firewall, IPS and Application Detection

Generall Firewall Configuration

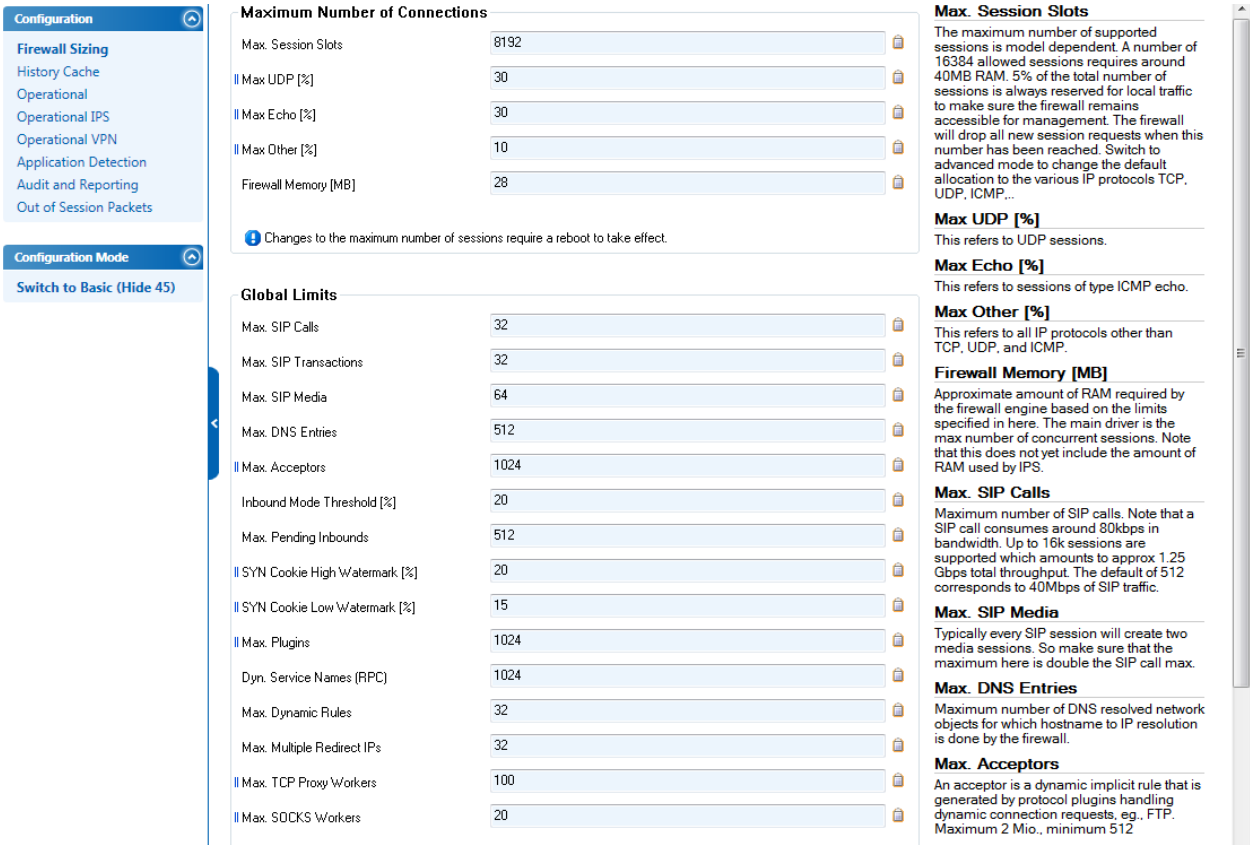
The ***General Firewall Configuration*** page was completely reworked in order to enhance usability and intuitive administration.

The Global Limits screen was renamed to ***Firewall Sizing***. The Session Limits and Memory Settings section from within the old Global Limits screen were moved to the Firewall Sizing screen. The Access Cache Settings in Global Limits were moved to the new ***History Cache*** screen. The Operational screen was split into ***Operational***, ***Operational IPS*** and ***Operational VPN***. In addition, the help comments on the right hand side were vastly improved to provide even better configuration support.



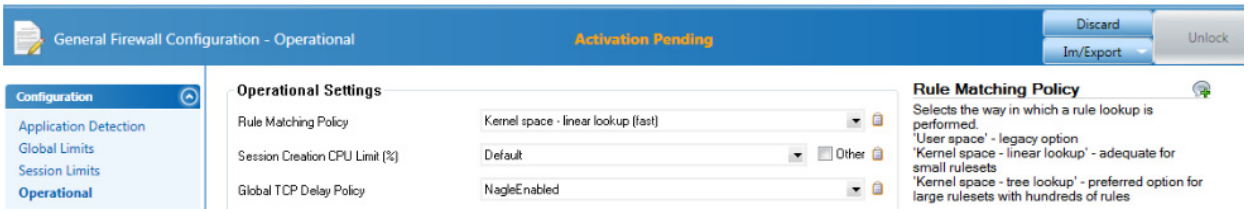
The ***General Firewall Configuration*** as well as all configuration comments were completely reworked in order to allow for more intuitive configuration and administration.

In addition, rarely used settings were moved into the ***Advanced*** view.


Configuration
Firewall Sizing
History Cache
Operational
Operational IPS
Operational VPN
Application Detection
Audit and Reporting
Out of Session Packets
Configuration Mode
Switch to Basic (Hide 45)
Maximum Number of Connections
Max. Session Slots 8192
Max UDP [%] 30
Max Echo [%] 30
Max Other [%] 10
Firewall Memory [MB] 28
Changes to the maximum number of sessions require a reboot to take effect.
Global Limits
Max. SIP Calls 32
Max. SIP Transactions 32
Max. SIP Media 64
Max. DNS Entries 512
Max. Acceptors 1024
Inbound Mode Threshold [%] 20
Max. Pending Inbounds 512
SYN Cookie High Watermark [%] 20
SYN Cookie Low Watermark [%] 15
Max. Plugins 1024
Dyn. Service Names (RPC) 1024
Max. Dynamic Rules 32
Max. Multiple Redirect IPs 32
Max. TCP Proxy Workers 100
Max. SOCKS Workers 20
Max. Session Slots
The maximum number of supported sessions is model dependent. A number of 16384 allowed sessions requires around 40MB RAM. 5% of the total number of sessions is always reserved for local traffic to make sure the firewall remains accessible for management. The firewall will drop all new session requests when this number has been reached. Switch to advanced mode to change the default allocation to the various IP protocols TCP, UDP, ICMP,..
Max UDP [%]
This refers to UDP sessions.
Max Echo [%]
This refers to sessions of type ICMP echo.
Max Other [%]
This refers to all IP protocols other than TCP, UDP, and ICMP.
Firewall Memory [MB]
Approximate amount of RAM required by the firewall engine based on the limits specified in here. The main driver is the max number of concurrent sessions. Note that this does not yet include the amount of RAM used by IPS.
Max. SIP Calls
Maximum number of SIP calls. Note that a SIP call consumes around 80kbps in bandwidth. Up to 16k sessions are supported which amounts to approx 1.25 Gbps total throughput. The default of 512 corresponds to 40Mbps of SIP traffic.
Max. SIP Media
Typically every SIP session will create two media sessions. So make sure that the maximum here is double the SIP call max.
Max. DNS Entries
Maximum number of DNS resolved network objects for which hostname to IP resolution is done by the firewall.
Max. Acceptors
An acceptor is a dynamic implicit rule that is generated by protocol plugins handling dynamic connection requests, eg., FTP. Maximum 2 Mio., minimum 512

General Firewall: Kernel Ruleset Renamed to Rule Matching Policy

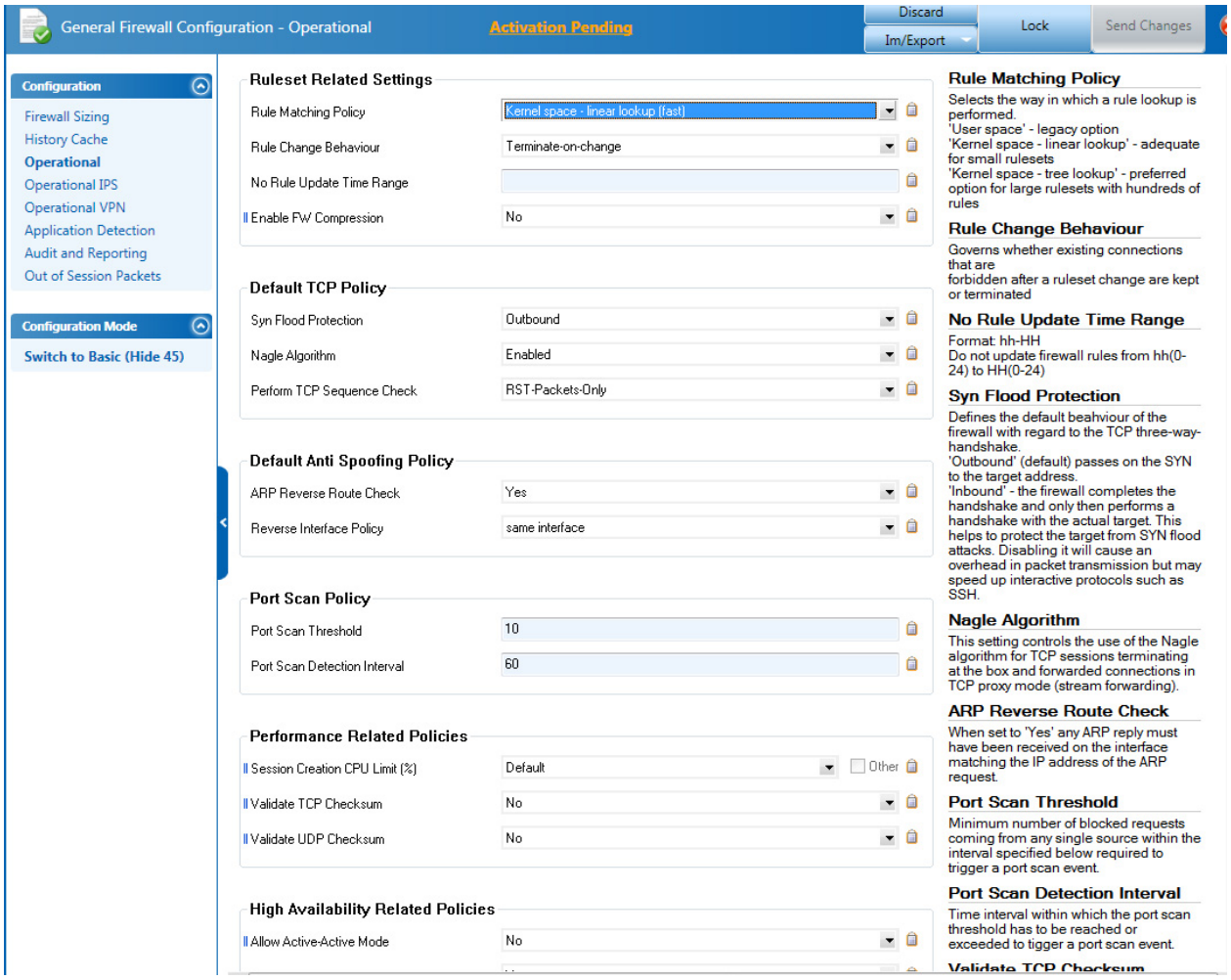
The Kernel Ruleset with its options no, yes or accelerated was renamed to ***Rule Matching Policy*** with its options ***User Space***, ***Kernel Space - linear lookup*** and ***Kernel Space – tree lookup***. By default, the firewall rule matching policy is now set to ***Kernel Space – tree lookup*** for new installations.


General Firewall Configuration - Operational
Activation Pending
Discard
Im/Export
Unlock
Configuration
Application Detection
Global Limits
Session Limits
Operational
Operational Settings
Rule Matching Policy Kernel space - linear lookup (fast)
Session Creation CPU Limit [%] Default Other
Global TCP Delay Policy NagleEnabled
Rule Matching Policy
Selects the way in which a rule lookup is performed.
'User space' - legacy option
'Kernel space - linear lookup' - adequate for small rulesets
'Kernel space - tree lookup' - preferred option for large rulesets with hundreds of rules

General Firewall: Operational

The ***Operational*** page of the ***General Firewall Configuration*** was reworked to group related entries. Help comments have been improved. Configuration items related to IPS and VPN were moved to separate

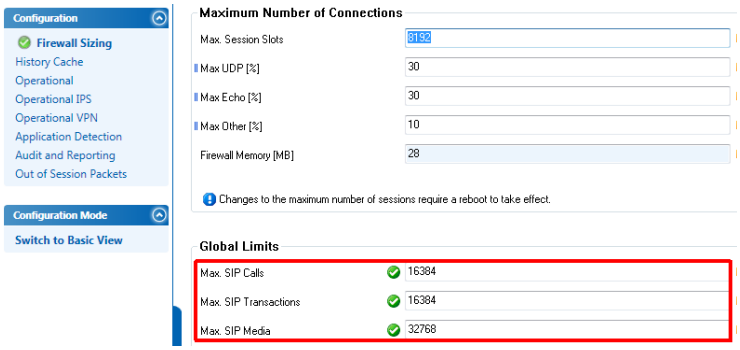
screens named ***Operational IPS*** and ***Operational VPN***.


General Firewall Configuration - Operational
Activation Pending
Discard
Im/Export
Lock
Send Changes
Configuration
Firewall Sizing
History Cache
Operational
Operational IPS
Operational VPN
Application Detection
Audit and Reporting
Out of Session Packets
Configuration Mode
Switch to Basic (Hide 45)
Ruleset Related Settings
Rule Matching Policy
Kernel space - linear lookup (fast)
Rule Change Behaviour
Terminate-on-change
No Rule Update Time Range
Enable FW Compression
No
Default TCP Policy
Syn Flood Protection
Outbound
Nagle Algorithm
Enabled
Perform TCP Sequence Check
RST-Packets-Only
Default Anti Spoofing Policy
ARP Reverse Route Check
Yes
Reverse Interface Policy
same interface
Port Scan Policy
Port Scan Threshold
10
Port Scan Detection Interval
60
Performance Related Policies
Session Creation CPU Limit [%]
Default
Other
Validate TCP Checksum
No
Validate UDP Checksum
No
High Availability Related Policies
Allow Active-Active Mode
No
Rule Matching Policy
Selects the way in which a rule lookup is performed.
'User space' - legacy option
'Kernel space - linear lookup' - adequate for small rulesets
'Kernel space - tree lookup' - preferred option for large rulesets with hundreds of rules
Rule Change Behaviour
Governs whether existing connections that are
forbidden after a ruleset change are kept or terminated
No Rule Update Time Range
Format: hh-HH
Do not update firewall rules from hh(0-24) to HH(0-24)
Syn Flood Protection
Defines the default beahviour of the firewall with regard to the TCP three-way-handshake.
'Outbound' (default) passes on the SYN to the target address.
'Inbound' - the firewall completes the handshake and only then performs a handshake with the actual target. This helps to protect the target from SYN flood attacks. Disabling it will cause an overhead in packet transmission but may speed up interactive protocols such as SSH.
Nagle Algorithm
This setting controls the use of the Nagle algorithm for TCP sessions terminating at the box and forwarded connections in TCP proxy mode (stream forwarding).
ARP Reverse Route Check
When set to 'Yes' any ARP reply must have been received on the interface matching the IP address of the ARP request.
Port Scan Threshold
Minimum number of blocked requests coming from any single source within the interval specified below required to trigger a port scan event.
Port Scan Detection Interval
Time interval within which the port scan threshold has to be reached or exceeded to tigger a port scan event.

General Firewall: Maximum Number of Allowed SIP Sessions

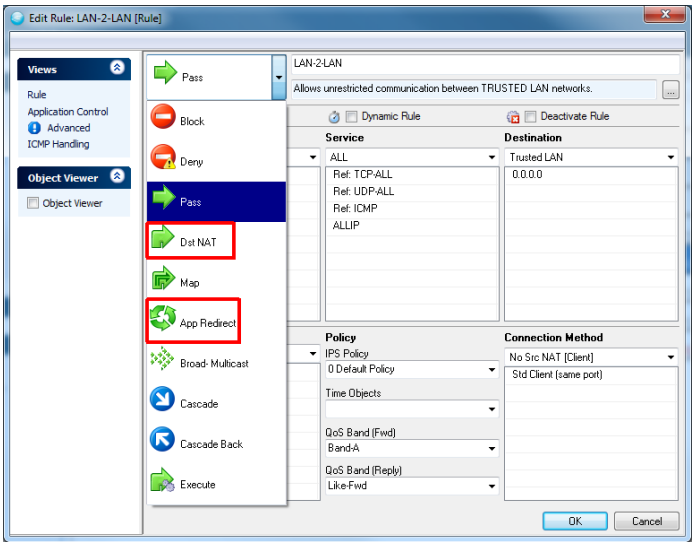
The maximum number of SIP sessions was increased. This is found in ***General Firewall Configuration > Firewall Sizing***.

- ***Max. SIP Calls: 16.384***
- ***Max. SIP Transactions: 16.384***
- ***Max SIP Media: 32.768***



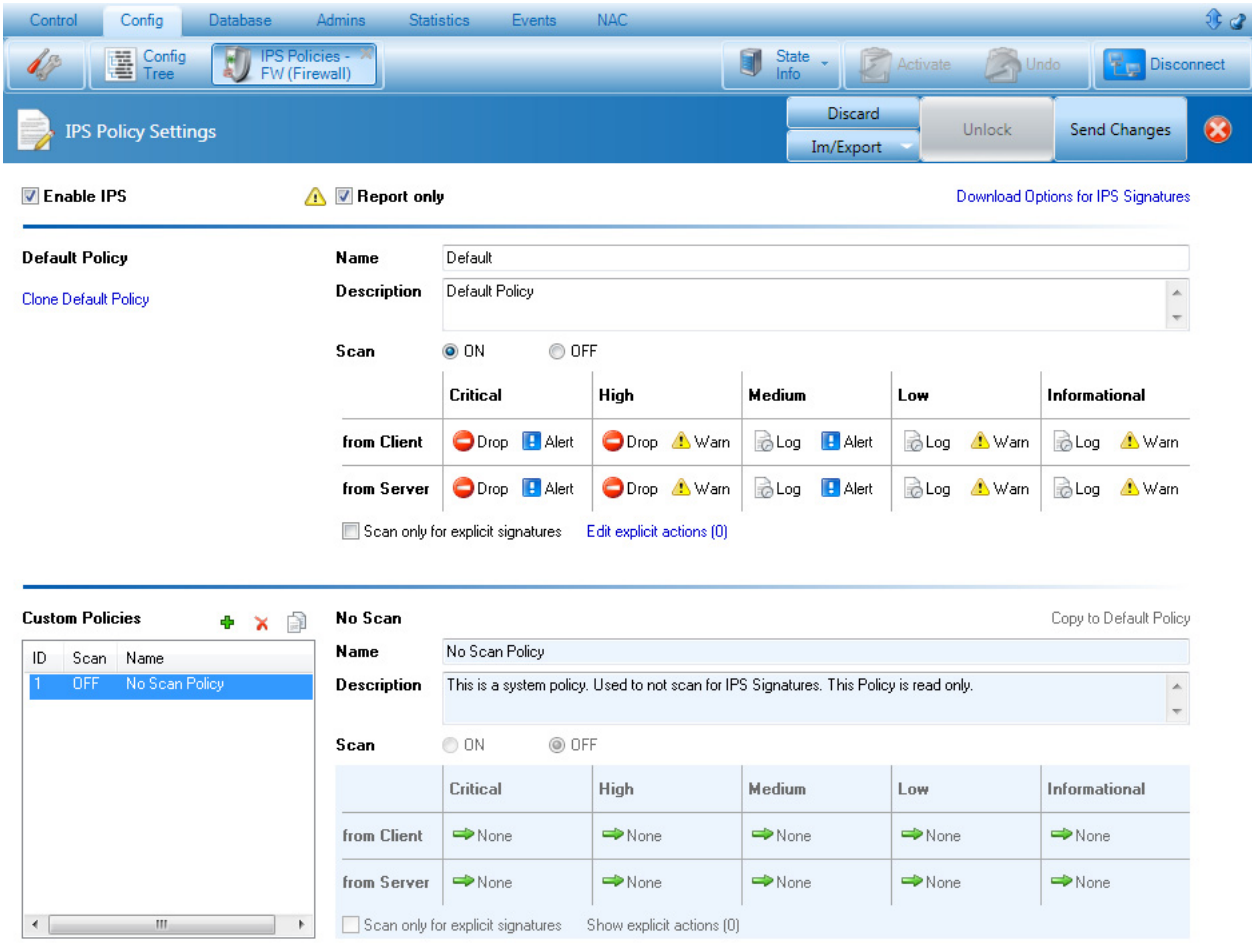
Firewall Rule Editor Usability Improvements

In order to simplify configuration, the legacy action types REDIRECT and REDIRECT OBJECT were replaced by the the new ***Dst NAT*** action type.



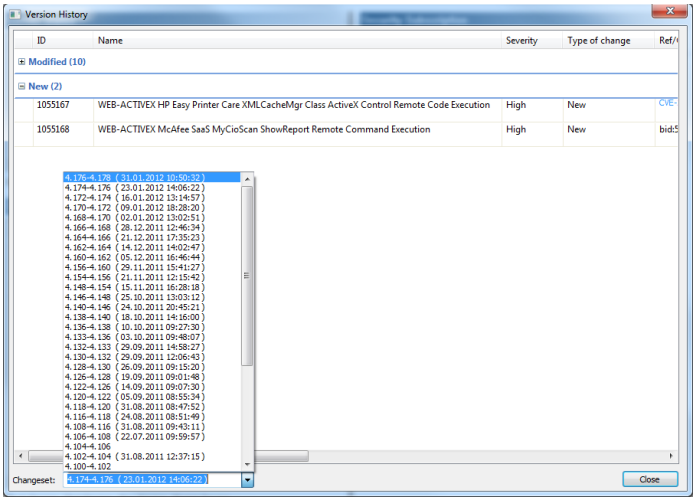
IPS Default Read Only

The default working mode of the Barracuda IPS engine was changed to ***Report only***. This behavior is only valid for newly installed Barracuda NG Firewall units. Upgrades from previous release will not be affected by this default change.

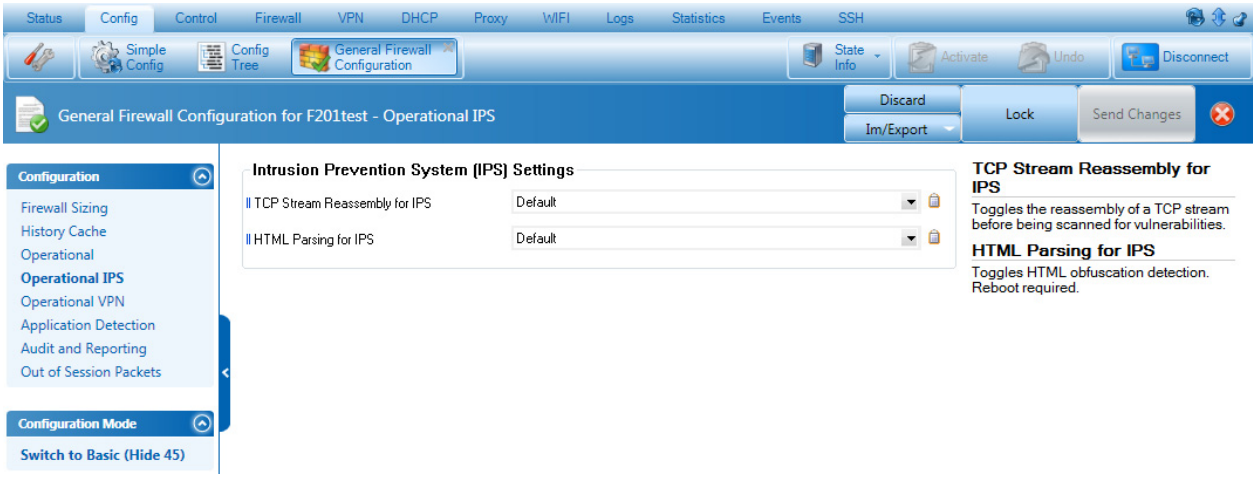


IPS Interface Improvements

The ***IPS Version History*** view now also displays the timestamp if a new IPS signature version was installed.



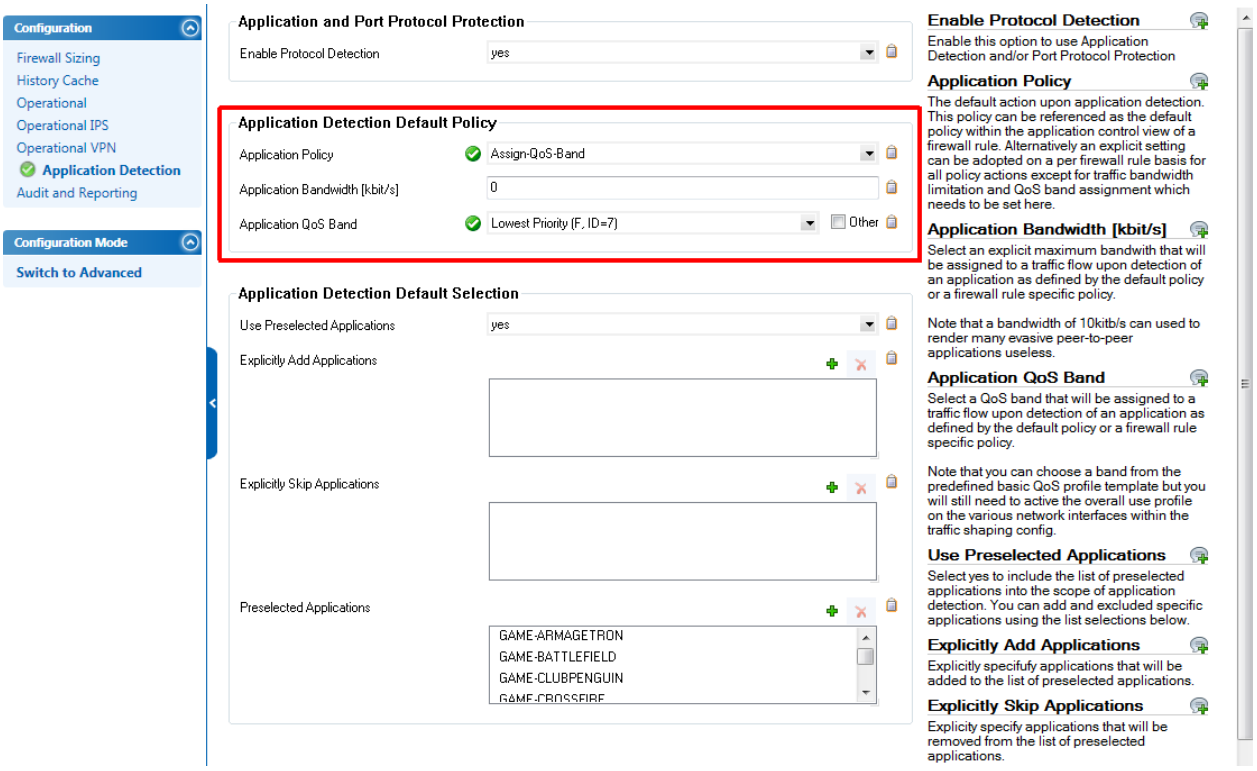
IPS advanced settings ***TCP Stream Reassembly for IPS*** and ***HTML Parsing for IPS*** are now found within the newly introduced ***Operational IPS*** section in the ***Advanced*** view of the ***General Firewall Configuration*** settings.



QoS and Application Detection

With firmware release version 5.2.3, it is now possible to use configured QoS schemes, previously referred to as Traffic Shaping Schemes, as ***Application Detection Default Policy*** by using the newly introduced ***Assign QoS Band*** policy. The help comments on the right hand side of the UI were updated

in order to improve usability and ease-of-use.


Configuration
Firewall Sizing
History Cache
Operational
Operational IPS
Operational VPN
Application Detection
Audit and Reporting
Configuration Mode
Switch to Advanced
Application and Port Protocol Protection
Enable Protocol Detection
yes
Application Detection Default Policy
Application Policy
Assign-QoS-Band
Application Bandwidth [kbit/s]
0
Application QoS Band
Lowest Priority (F, ID=7)
Other
Application Detection Default Selection
Use Preselected Applications
yes
Explicitly Add Applications
Explicitly Skip Applications
Preselected Applications
GAME-ARMAGETRON
GAME-BATTLEFIELD
GAME-CLUBPENGUIN
GAME-CROSSFIRE
Enable Protocol Detection
Enable this option to use Application Detection and/or Port Protocol Protection
Application Policy
The default action upon application detection. This policy can be referenced as the default policy within the application control view of a firewall rule. Alternatively an explicit setting can be adopted on a per firewall rule basis for all policy actions except for traffic bandwidth limitation and QoS band assignment which needs to be set here.
Application Bandwidth [kbit/s]
Select an explicit maximum bandwith that will be assigned to a traffic flow upon detection of an application as defined by the default policy or a firewall rule specific policy.
Note that a bandwidth of 10kitb/s can used to render many evasive peer-to-peer applications useless.
Application QoS Band
Select a QoS band that will be assigned to a traffic flow upon detection of an application as defined by the default policy or a firewall rule specific policy.
Note that you can choose a band from the predefined basic QoS profile template but you will still need to active the overall use profile on the various network interfaces within the traffic shaping config.
Use Preselected Applications
Select yes to include the list of preselected applications into the scope of application detection. You can add and excluded specific applications using the list selections below.
Explicitly Add Applications
Explicitly specifufy applications that will be added to the list of preselected applications.
Explicitly Skip Applications
Explicity specify applications that will be removed from the list of preselected applications.

Web Proxy

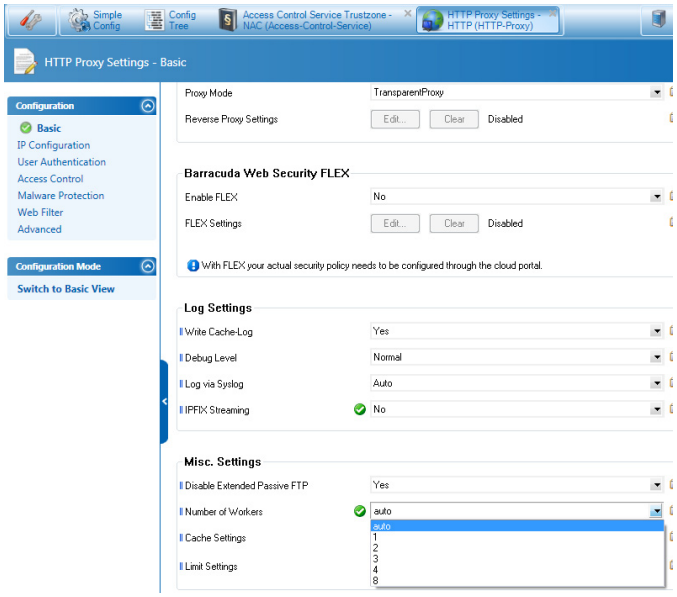
Update of Underlying Squid Engine to Support Multiple Cores

Starting with firmware release version 5.2.3, the underlying squid engine was upgraded from 3.1.06 to 3.2.0.7. This introduces support for multiple CPU cores and results in significant improvements in proxy performance on Barracuda NG Firewall units with multiple CPUs or multiple CPU cores (F400 and higher). By default (***auto***) as many squid processes (***workers***) are started as logical CPU cores are available up to a maximum of 8. This setting may be adjusted in the ***HTTP Proxy*** settings within the ***Advanced*** view, however, Barracuda Networks recommends to leave the value at ***auto***.

Note

This feature has previously already been introduced in hotfix 438 for firmware version 5.2.2.

The figure below shows the number of proxy worker processes for multicore machines (recommended: ***auto***).)

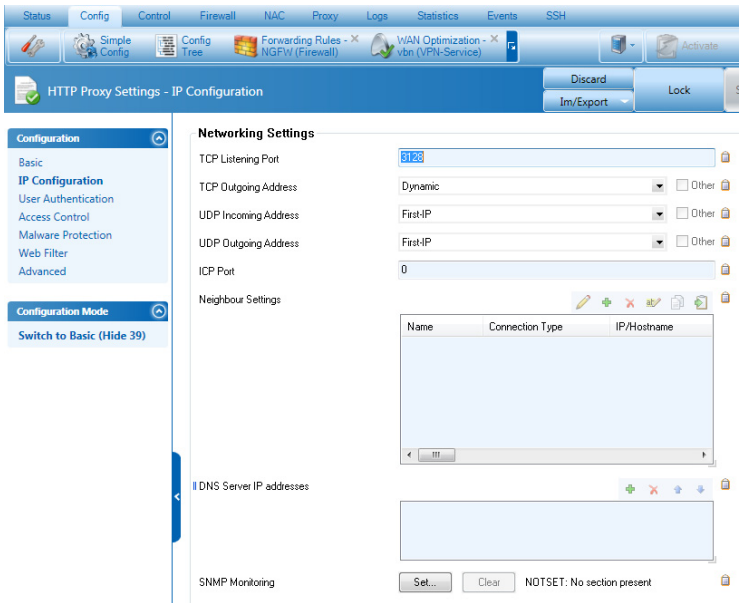


Dedicated DNS Settings for Proxy

With firmware release version 5.2.3, the proxy may utilize its own set of DNS IP addresses.

Note

Once a DNS IP address is set, the proxy will not fall back to the system settings if the DNS server(s) assigned to it become unreachable. This setting is only visible in ***Advanced*** view.

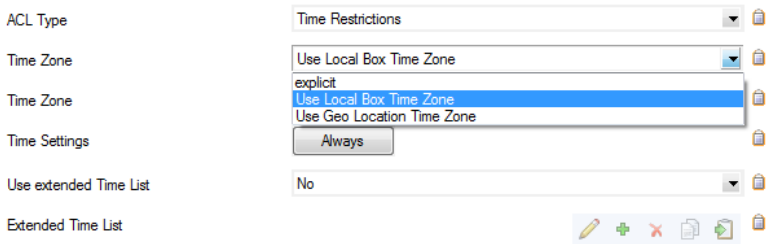


Proxy ACL Based on Geo Location Time Zone

Starting with firmware release version 5.2.3, time-based proxy access control lists (ACLs) can be set up so that they refer to the actual time zone of the geo location of the Barracuda NG Firewall unit. The geo location can be set in the ***Box Properties*** section of centrally managed units.

Note

This feature is not available for unmanaged (stand-alone) units.



Virus Scanner (Malware Protection)

Simplification of Virus Scanner Configuration

Starting with firmware version 5.2.3, logically related configuration items were grouped together. Various less often used fields are now only displayed if ***Advanced*** mode is selected. The help comments where extended.

The Virus Scanner Service defaults were optimized so that the actual service configuration must no longer be opened for most of the time upon service creation.

VPN and WAN Optimization

XAUTH Authentication Support

Starting with firmware release version 5.2.3, the Barracuda NG Firewall now also supports the IPsec XAUTH authentication standard. This allows for creating VPN tunnels between Barracuda NG Firewall units and mobile devices, e.g. iOS devices, which are using Cisco IPsec clients.

One Time Password (OTP) Support for SSL VPN

Firmware release version 5.2.3 introduces OTP support via RADIUS authentication also for SSL VPN.

Simplification of VPN Service Configuration

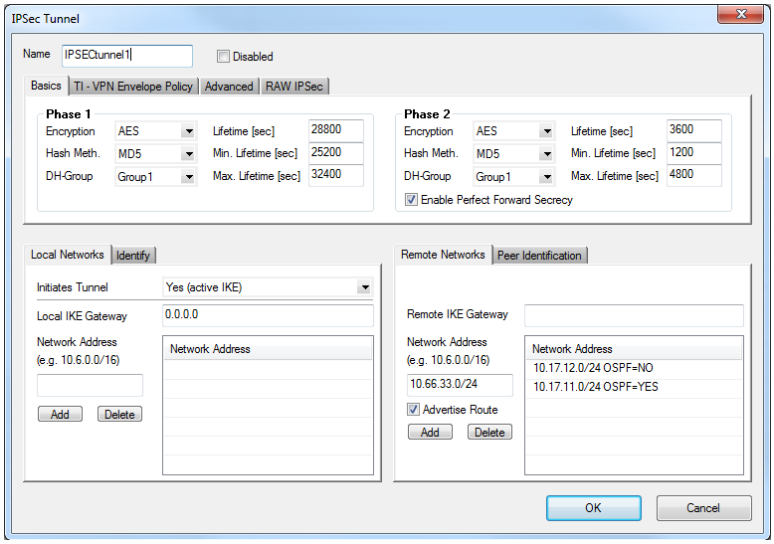
Starting with firmware version 5.2.3, several tags inside the VPN service configuration are renamed to match industry standards.

Advertise Remote Network Routes Via OSPF/RIP for IPSEC Site-to-Site

Starting with firmware version 5.2.3, also the remote networks of IPSEC-based site-to-site tunnels will be advertised via OSPF/RIP if the respective checkbox is marked accordingly.

Note

This feature is not yet available for VPN tunnels in the GTI Editor..



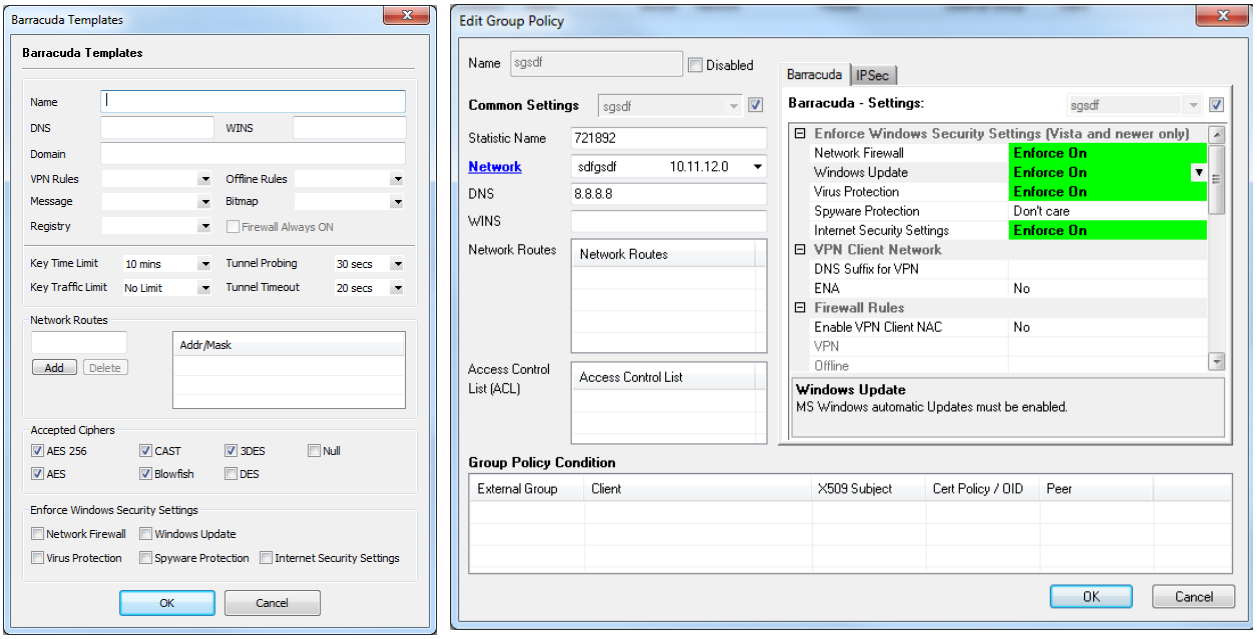
VPN Access Enforcement Based on Windows Security Center Settings

Starting with firmware release version 5.2.3, the settings configured within the Windows Security Center as available with Windows Vista and Windows 7 may be read and matched against a given policy before any access to the network via VPN is granted.

This enforcement can be defined per client as well as per group template.

Note

This feature is part of the standard VPN implementation and does therefore not require a SSL VPN & NAC license..



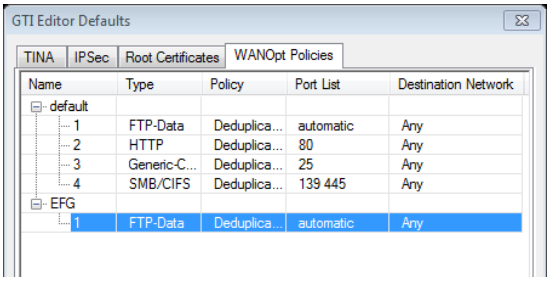
WAN Optimization

Starting with firmware release version 5.2.3, the ***Deduplication Dictionary Settings*** were moved into the ***Advanced*** view. In general, all WAN optimization related entries in the configuration were renamed from "WAN compression" or "WANcomp" to "WAN optimization" and "WANopt". The WANOpt policy “GLD” (=generic large dictionary) was renamed to "Deduplication".

WAN Optimization in GTI

Activation and configuration of WAN optimization was added to the GTI editor. WAN optimization can now be configured within the new ***WANOpt Policies*** tab in the ***GTI Editor Defaults*** screen. Individual GTI groups can be assigned a default WAN optimization policy that is then applied to all VPN tunnels in

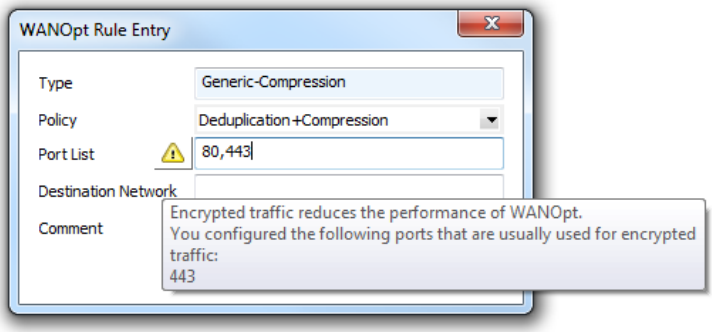
that group. Additionally, WAN optimization policies may be set per VPN Tunnel.



WAN Optimization: Warning Display for Encrypted Ports

If one of the ports listed in the table below is selected within a WAN optimization rule, a warning is indicated to indicate that using encrypted traffic for WAN optimization is not recommended as it will significantly reduce WAN optimization performance because the cache dictionary is filled with data that will never have a counterpart on the other side of the tunnel.

Port	Protocol
22	ssh
443	https
688, 801, 805, 807, 808, 809, 810, 811, 815, 816, 843, 844, 845, 880, 888	Management for NG Admin and CC
636	ldap over SSL
706	Secure Internet Live Conferencing
989, 990, 991, 992, 993, 994, 995	FTP/Telnet/IMAP/IRC/POP3 over SSL
1194	OpenVPN
0	terminating array



WAN Optimization and VPN Tunnel Compression Compatibility

With firmware release versions 5.2.0 to 5.2.2, it was possible to configure a VPN transport with stream or packet based compression while at the same time activating WAN optimization (then called WAN

compression). However, compressing a packet twice results in undesirable side effects such as performance overhead and additional latency and should therefore generally be avoided.

Firmware release version 5.2.3 introduces two changes to resolve the situation described above.

If WAN optimization is enabled for a transport, a potentially configured stream compression is automatically disabled. The GUI will then display a corresponding warning.

Furthermore, if WAN optimization is enabled for a transport and packet compression is enabled as well, packet compression is disabled for WAN optimization traffic, but not for other traffic using the same transport. There is no visual indication in this case.

WAN Optimization : Show Compression Statistics

With firmware release version 5.2.3, the compression for every transport can be displayed within the CLI using the `ktinactrl wanopt stat` command. For future firmware releases, this information is scheduled to be provided within the GUI.

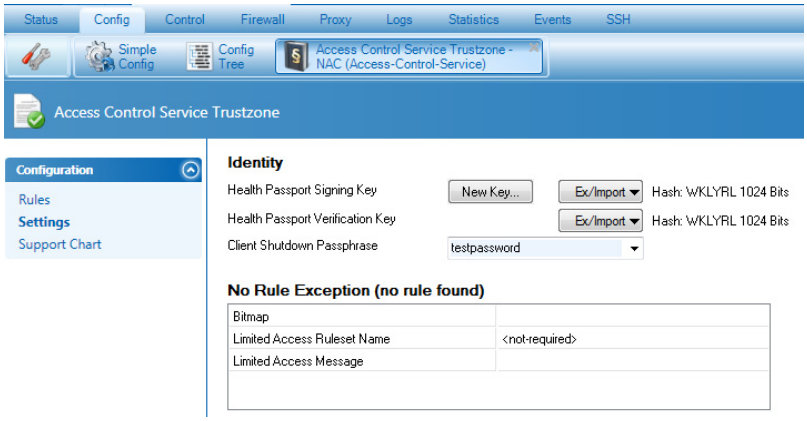
```
[root@F800-2:~]# ktinactrl wanopt stat
Transport 0 'FW2FW-HQTina' uses wanopt policy 'GLD-only'
        Rule # 0: Compression ratio inbound=96% outbound= 0% total=96%
        Rule # 1: Compression ratio inbound= 0% outbound= 0% total= 0%
        Rule # 2: Compression ratio inbound= 0% outbound= 0% total= 0%
        Rule # 3: Compression ratio inbound= 0% outbound= 0% total= 0%
        Rule # 4: Compression ratio inbound= 0% outbound= 0% total= 0%
        Overall : Compression ratio inbound=96% outbound= 0% total=96%
[2012-02-14 14:04 UTC] [-root shell-] [-Barracuda Networks-]
[root@F800-2:~]#
```

SSL VPN & NAC: Centrally Managed Password for NAC Deactivation

Starting with firmware release version 5.2.3, the password to turn off the NAC client (3.0 and up) can be centrally managed from with the ***Access Control Service*** configuration.

Note

A centrally managed password for NAC deactivation only applies to local NAC installations, but not to NAC accessing the network via VPN.



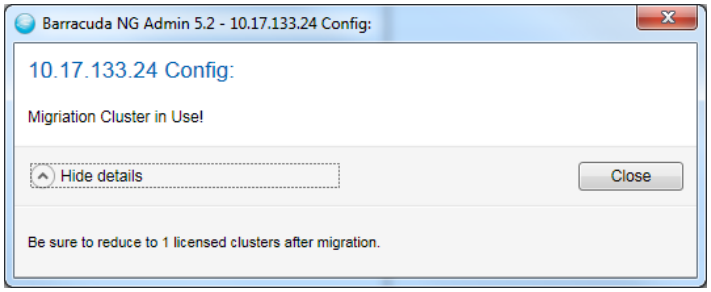
Control Center Related Changes

RCS Now Logs Changes Made Via GTI Editor Changes

Starting with firmware release version 5.2.3, all changes done within the Graphical VPN Tunnel Editor Interface (GTI Editor) will be stored in the RCS history.

Additional Migration Cluster

Even if the license for the Barracuda NG Control Center (e.g. C400 or VC400) only includes one single configuration cluster, an additional cluster for migration purposes may be created. This cluster will always be named ***migrate*** and a benign error message will appear for every login or connecting attempt to the Barracuda NG Control Center. Any attempt to create an additional third cluster will fail.


Barracuda NG Admin 5.2 - 10.17.133.24 Config:
10.17.133.24 Config:
Migriation Cluster in Use!
Hide details
Close
Be sure to reduce to 1 licensed clusters after migration.

Other

Box Properties Configuration Node

Starting with firmware release version 5.2.3, the ***Box Properties*** configuration was reworked to be more intuitive to use. Help texts were as well improved. Certain less-often used configuration fields were moved to the newly created ***Advanced*** view.

The ***Appliance Name*** and ***Unique Appliance Name*** fields are no longer displayed on unmanaged (standalone) units.

A new ***Software Firewall (SF)*** appliance model was added to support special cases of licensing on legacy hardware or commodity hardware.

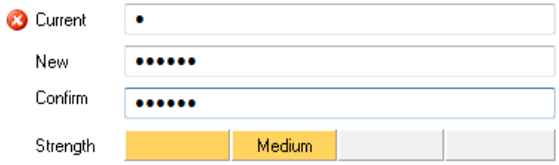
Password Strength Meter

Firmware release version 5.2.3 introduces a password strength meter to displaying the effectiveness of newly set passwords during their creation. The password strength check rates as follows:

- ***1 point for length > 7***
- ***2 points for length > 15***
- ***1 point for a small character***
- ***2 points for 2 different small characters***
- ***1 point for a capital character***
- ***2 points for 2 different capital characters***
- ***1 point for a digit***
- ***2 points for 2 different digits***
- ***1 point for a non-alpha num symbol***
- ***2 points for 2 different non-alpha num symbols***

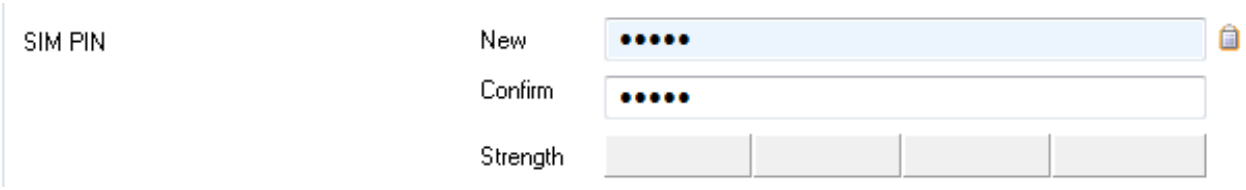
1-4 points is rated ***weak***, 5 to 7 points is rated ***medium***, 8 to 9 points is rated ***strong***, 10 points is rated ***best***.

The sample figure below shows what's displayed if a password is rated medium:



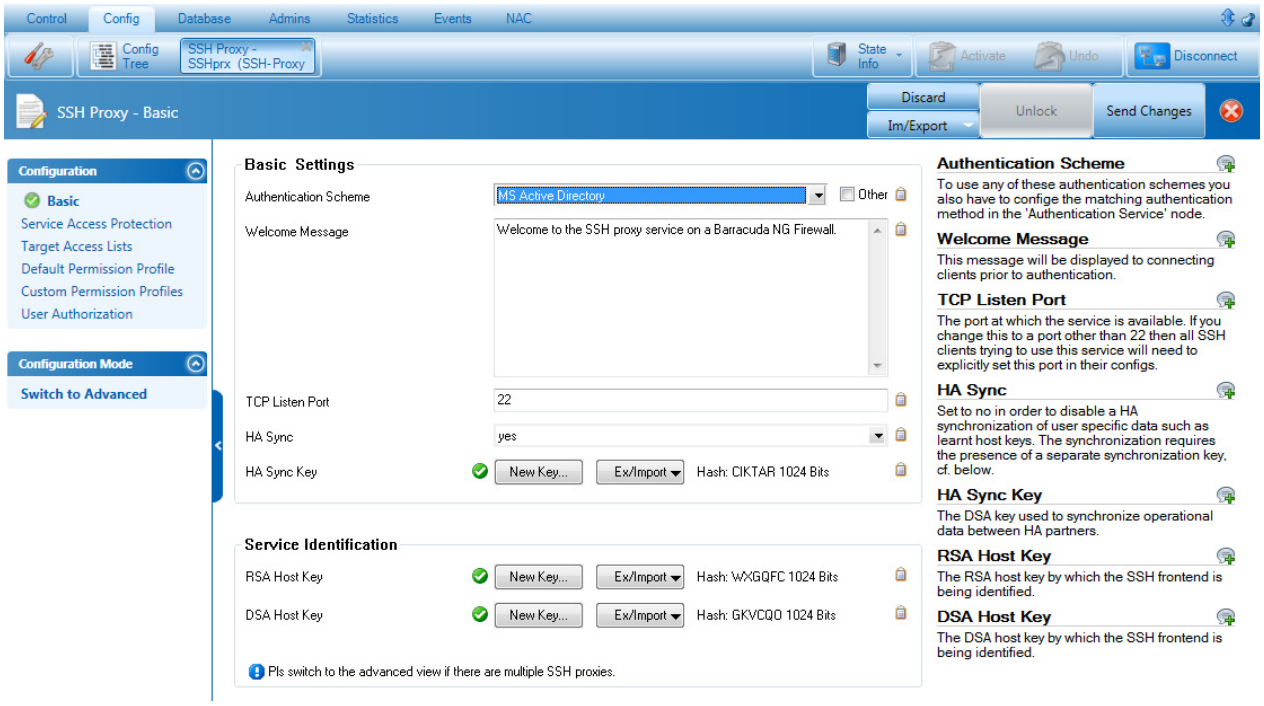
Updated Password Entry Configuration Object

Starting with firmware release version 5.2.3, wherever in the Barracuda NG Firewall configuration a password needs to be set by the user via Barracuda NG Admin, the Current Password field is removed. Instead, ***New*** and ***Confirm*** fields are displayed and used for password entry. If a password has already been set before, the current password will be displayed there in a dotted and obfuscated manner.

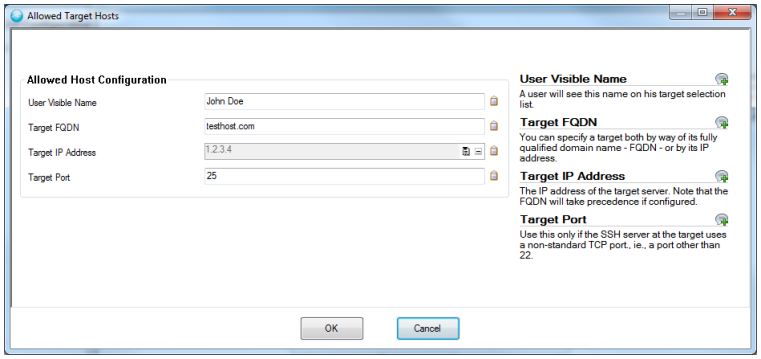


SSH Proxy:

Starting with firmware release version 5.2.3, the menu structure, the configuration handling and the comments within the ***SSH Proxy*** user interface were completely reworked and simplified.


Control
Config
Database
Admins
Statistics
Events
NAC
Config Tree
SSH Proxy - SSHprx (SSH-Proxy
State Info
Activate
Undo
Disconnect
SSH Proxy - Basic
Discard
Im/Export
Unlock
Send Changes
Configuration
Basic
Service Access Protection
Target Access Lists
Default Permission Profile
Custom Permission Profiles
User Authorization
Configuration Mode
Switch to Advanced
Basic Settings
Authentication Scheme
MS Active Directory
Other
Welcome Message
Welcome to the SSH proxy service on a Barracuda NG Firewall.
TCP Listen Port
22
HA Sync
yes
HA Sync Key
New Key...
Ex/Import
Hash: CIKTAR 1024 Bits
Service Identification
RSA Host Key
Hash: WXGQFC 1024 Bits
DSA Host Key
Hash: GKVCQO 1024 Bits
Pls switch to the advanced view if there are multiple SSH proxies.
Authentication Scheme
To use any of these authentication schemes you also have to confige the matching authentication method in the 'Authentication Service' node.
Welcome Message
This message will be displayed to connecting clients prior to authentication.
TCP Listen Port
The port at which the service is available. If you change this to a port other than 22 then all SSH clients trying to use this service will need to explicitly set this port in their configs.
HA Sync
Set to no in order to disable a HA synchronization of user specific data such as learnt host keys. The synchronization requires the presence of a separate synchronization key, cf. below.
HA Sync Key
The DSA key used to synchronize operational data between HA partners.
RSA Host Key
The RSA host key by which the SSH frontend is being identified.
DSA Host Key
The DSA host key by which the SSH frontend is being identified.

There is a new configuration option for outbound compression named ***always use***. The user query for compression is therefore no longer needed. In addition, it is now possible to configure a non-standard port, other than port 22, for predefined target hosts.


Allowed Target Hosts
Allowed Host Configuration
User Visible Name
John Doe
Target FQDN
testhost.com
Target IP Address
1.2.3.4
Target Port
25
User Visible Name
A user will see this name on his target selection list.
Target FQDN
You can specify a target both by way of its fully qualified domain name - FQDN - or by its IP address.
Target IP Address
The IP address of the target server. Note that the FQDN will take precedence if configured.
Target Port
Use this only if the SSH server at the target uses a non-standard TCP port., ie., a port other than 22.
OK
Cancel

Simplification and Renaming of Server Configuration

Starting with firmware release version 5.2.3, the ***Virtual Server*** configuration was reworked to be more intuitive and conform to industry naming standards. Additionally, the help comments on the right side were clarified and expanded.

Create PAR Files for Single Units on NG Control Center

Firmware version 5.2.3 now supports the creation of PAR files for individual units via the command line interface on a Barracuda NG Control Center.

Related Docs

See the **Barracuda NG Firewall CLI Guide** for in-depth information on this feature. The CLI Guide is downloadable through **http://barracuda.com/doc**.

New Semantics

Table 1–3 Different Administrative Configurations

GUI Location	Old	New
Box Properties	Legacy Appliance Model Settings	(moved to ***Advanced*** mode)
	Detect Appl. Model Mismatch	Moved to Operational screen
	Appliance Name	(no longer displayed for standalone units)
	Unique Appliance Name	(no longer displayed for standalone units)
Box Network > Trunking	Ethernet Trunks	Ethernet Bundles (own menu)
	Virtual Interface	Bundled Interface
	Trunked Interfaces	Bundled Interfaces
	Operation Mode: Bundle	Operation Mode: Balance-RR
	Operation Mode: Fallback	Operation Mode: Active-Backup
	Operation Mode: XOR	Operation Mode: Balance-XOR
	Operation Mode: LinkAggregation	Operation Mode: 802.3ad LinkAggregation
Box Network > Virtual LANs	Hosting Interface	Physical VLAN Interface
	VLAN ID	VLAN Tag
Box Network > Routing	Policy Based Routing	Source-based Routing

Table 1–3 Different Administrative Configurations

GUI Location	Old	New
Box Network > UMTS / 3G	APN Name	Access Point Name (APN)
	Active 2nd Channel	Active GSM Channel
	Network Realm	Trust Level
	Route Preference Number	Route Metric
	Register in standby	(moved to ***Advanced*** mode)
	Modem Error Policy	(moved to ***Advanced*** mode)
Firewall Rule Editor	Redirect	Dst NAT
	Redirect Object	Dst NAT
	Local Redirect	App Redirect
	Local Redirect Object	App Redirect
	2-way	Bi-Directional
	Dynamic Src NAT [Proxydyn]	Source-based NAT
	Fwd Shaping	QoS Band (Fwd)
	Revf Shaping	QoS Band (Reply)
Firewall > Ruleset > Proxy ARPs > Edit / Create	noext	"noext" in ProxyARP creation window removed
General Firewall Settings	Operational: Kernel Ruleset	Operational: Rule Matching Policy
	Operational: Kernel Ruleset values no, yes, accelerated	User Space, Kernel Space-linear lookup, Kernel Space - tree lookup
	Global Limits	Firewall Sizing
	Access Cache Settings	History Cache Limits
	ACPF Memory [MB]	Firewall Memory [MB]
Network Object Groups	Local	Static
	Global	Shared
Connection Object (Edit / Create)	New Standard...	New Connection...
Traffic Shaping	Virtual Shaping Tree	QoS Profile
	Shaping Connector	QoS Band
	Fwd Shaping	QoS Band (Fwd)
	Rev Shaping	QoS Band (Reply)
VPN	WAN Compression	WAN Optimization
VPN Settings	Personal Networks	Client Networks
VPN Site to Site	WANcomp Policies	WANOpt Policies
VPN Site to Site > WANOpt Policies	GLD	Deduplication

Table 1–3 Different Administrative Configurations

GUI Location	Old	New
VPN Site to Site > IPSEC	Local Address	Local IKE Gateway
	Remote Address	Remote IKE Gateway
VPN Site to Site > IPSec Identity	Shared Passphrase	Shared Secret
	Aggressive-ID	The Aggressive-ID field now accepts alphanumeric characters as well as the following special characters: `.!#$%&'*+-/=?^_`{|}~@`
VPN > IPSec Tunnels > Local Networks	Call direction	Initiates Tunnel
	Active	Yes (active IKE)
	Passive	No (passive IKE)
VPN > IPSec Tunnels > Basics > Phase 2	none	Enable Perfect Forwarding Secrecy (**new** checkbox)
URL Filter Service	ISS Proventia Web Filter	URL Filter
	Disable Service (default value: ***no***)	Enable Service (default value: ***yes***)
Virus Scanner Service	Disable Service (default value: ***no***)	Enable Service (default value: ***yes***)
	Enable Avira	Enable Avira Engine
	Enable ClamAV	Enable ClamAV Engine
	Max. file RAM usage [MB]	Max. RAM Cache [MB]
	Max. Num. Workers	Max. Number of Workers (only visible in ***Advanced*** mode)
	Reporting	User Notification
	Updates	Update Handling
	Retries	Download Retries (only visible in ***Advanced*** mode)
	Avira Update settings	Download Server Addresses (merged with ClamAV Update settings, only visible in ***Advanced*** mode)
	ClamAV Update settings	Download Server Addresses (merged with Avira Update settings, only visible in ***Advanced*** mode)
	Avira (section)	Settings moved to either one of these new sections: Archive Scanning, Malware Coverage, Engine Specifics
	ClamAV (section)	Settings moved to either one of these new sections: Archive Scanning, Malware Coverage, Engine Specifics
	Streaming settings	Content Scanning

Table 1–3 Different Administrative Configurations

GUI Location	Old	New
Server Properties	General	Basic
	Description	(only visible in ***Advanced*** mode)
	First-IP (S1)	First-IP (IP1)
	Second-IP (S2)	Second-IP (IP2)
	Monitoring	Monitoring Policy
	Enable Monitoring on Secondary	Monitoring on backup Box
	IP Monitoring	Layer 3 Monitoring
	Interface Monitoring	Layer 2 Monitoring
	Scripts	Custom Scripts
Simple Config	Network	IP Configuration

What´s New with Barracuda NG Network Access Client 2.0 SP6?

Service Pack 6 for Barracuda NG Network Access Client 2.0 comes with a variety of improvements that are described below.

User Client Shutdown Password Centrally Manageable

The shutdown password can now be managed centrally from within the Access Control Service.

Immediate Health Validation on Demand

The ***Validate...*** link within the Health Agent Monitor triggers now immediate health validation.

Automatically Enable Quarantine, Receive Power Setting Notifications and Suppress Activity in Suspend Mode

The VPN service will now receive notifications for specific power setting events.

The new ***OnPowerRESUMEAutoQuarantine*** registry flag within ***HKEY_CURRENT_USER\Software\Phion\phionvpn\settings*** will trigger immediate loading of the quarantine ruleset in the Personal Firewall after waking up from standby or hibernate mode if set to ***1***.

Subsequently, the client will try to contact its Access Control Server in order to be able to deactivate the quarantine rule set again as soon as possible.

Additionally, it is possible to set ***OnPowerRESUMEQuarantineLoadOnly*** to ***1*** in order to load the quarantine ruleset **without** probing the active slots.

Furthermore, IP address monitoring and VPN system checks are now supressed while suspend mode is active.

Automatic VPN Termination on Unhealthy or Untrusted Client

An initially established VPN connection will now automatically be terminated again if the health check results in an unhealthy or untrusted state.

Default Quarantine Ruleset on Personal Firewall Start

The Personal Firewall is now able to start up with the activated quarantine ruleset.

Subsequently, the client will try to contact its Access Control Server in order to be able to deactivate the quarantine rule set again as soon as possible.

This mode can be activated by setting the ***UseDefaultQuarantineRuleset*** registry flag within ***HKEY_CURRENT_USER\Software\Phion\phionvpn\settings*** to ***1***.

VPN Probing Uses Windows Settings to Connect

The automatic VPN connection probing mechanism will now also detect respective Windows Explorer proxy settings in order to be able to use a proxy that might be configured there.

Regrouped Advanced Profile Settings

The ***Advanced*** settings in the ***VPN Profile*** dialog were regrouped for better usability.

VPN Profile Wizard X.509 Configuration Extended

The X.509 configuration within the VPN profile wizard now allows to choose either the ***User Store*** or the ***Local Computer Store*** for the certificate.

VPN DNS Domain Name Conflict Prevention

The client now helps preventing that a DNS suffix already configured on a different adapter is configured as a duplicate on a virtual adapter.

This prevents conflicts between VPN DNS domain names and external DNS domain names.

The following log message will be generated on connecting:

```
DNS Namespace exists on the Internet conflict with an organization's internal namespace.

To avoid networking problems the DNS Suffix will not be set on the Virtual Adapter!
```

```
Local DNS Suffix: company.com
VPN  DNS Suffix: company.com
```

Related Docs

This feature is compliant to the guidelines found at **http://support.microsoft.com/default.aspx?scid=kb;en-us;254680.**

Changed Multiple X.509 Certificates Handling

If multiple certificates are found, the client will now always try to find a valid certificate. However, this behavior can be suppressed through the ***VPN Profile***'s certificate selection dialog.

Access Control Server Certificate Check

An Access Control Server certificate check mechanism was implemented.

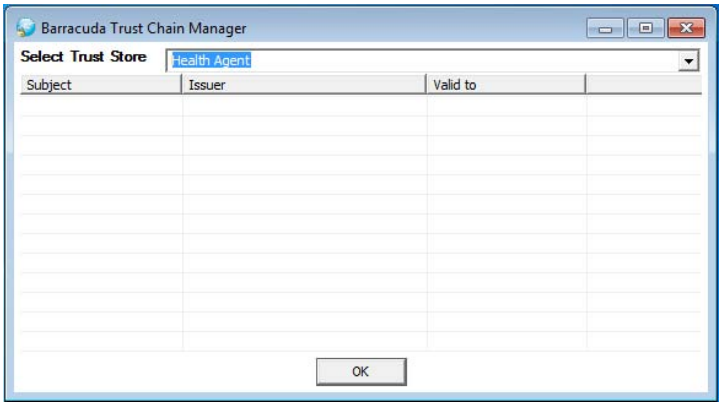
Health Agent Monitors Certification Authorities

The Health Agent now monitors the management of certification authorities.

Trust Chain Manager

Certificate management for the VPN Client was moved away from Barracuda NG VPN Control into a separate, new tool called Trust Chain Manager. With it, it's possible to manage certificates for the VPN connections as well as for checking the Access Control Service trust relationship.

The Access Control Server's X.509 certificates can be imported into the Trust Chain Manager as seen below.



The tool is executed from ***Start > Barracuda NG Network Access Client > Trust Chain Management*** or from the sub folder ***Utilities*** within the Barracuda NG Network Access Client installation folder. The executable file is named `TrustChain.exe`.

New Health Agent Registry Entry

A new registry configuration entry for the Health Agent was added:

HKEY_CURRENT_USER\Software\Phion\phionha\settings\QuarantineCountDownFirstTry: -1

This value will be used for the countdown at the very first validation. Default value is ***-1***.

VPN Profile Creation from a *.VPN File

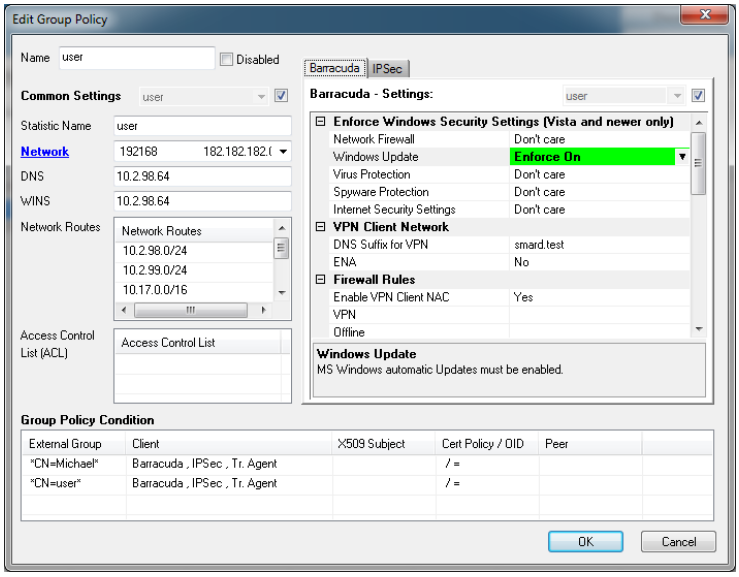
Clicking a file with the suffix '`vpn`' within the Windows Explorer will now create a VPN profile.

With Barracuda NG Admin 5.2.3, it is not yet possible to create such VPN profile files to be imported into the client. This will be implemented with a later version.

Aggregate Health State for Windows Security Provider

The Windows Action Center now provides security information from the Health Agent to the VPN server. Depending on the respective security values configured in Barracuda NG Admin, VPN

connections will either be allowed or denied.



Related Docs

This feature is compliant to the guidelines found at **http://windows.microsoft.com/en-US/windows7/Understanding-security-and-safer-computing**.

Registry Setting to Prevent OPSWAT Initialization

A configuration flag was added to the registry that prevents the OPSWAT engine from being initialized.

OpswatPreAllocation within ***HKEY_CURRENT_USER\Software\Phion\phionvpn\settings*** can be set to ***1*** (default value) in order to save system performance if OPSWAT functions are not needed.

Decreased Default MTU Size

Within the default ***Virtual Adapter*** settings, the maximum transmission unit (MTU) size was decreased to `1390` in order to reduce IP packet fragmentation.

Nagle's Algorithm Enabled for VPN Sockets

Nagle's algorithm is now enabled for VPN sockets per default.

Therefore, ***HKEY_CURRENT_USER\Software\Phion\phionvpn\settings\[DWORD]nodelay*** is set to ***0***. Set this value to ***1*** to disable Nagle's algorithm.

Registry Flag to Prevent Automatic X.509 Serial Number Updates

HKEY_CURRENT_USER\Software\Phion\phionvpn\settings\[DWORD]certSerialNumberAutoUpdate disables automatic updates to X.509 serial numbers when set to ***1***.

These updates will replace expired X.509 certificates by automatically importing replacement certificates from the store and assigning them the configured serial number. A certificate will be imported if subject and issuer match the old certificate. This registry setting prevents such updates.

Updated OPSWAT Libraries

OPSWAT has been updated to the latest release 3.5.324.2.

New Semantics

With firmware release version 5.2.3, certain terms were changed in order to become easier understandable and to match widespread industry standards. The table below lists all of these semantic changes.

Bugfixes Included with Barracuda NG Firewall 5.2.3

Barracuda NG Admin

Table 1–4 Barracuda NG Admin

Description
In rare cases, the Connection Object editor erroneously requested the user to select an object although this was actually not needed. This issue was fixed.
In rare cases, Barracuda NG Admin 5.2.2 was crashing in case loading config from the NG Control Center failed. This issue was fixed.
The ***Group VPN Settings > LDAP Attributes > IP Attribute Name*** length was erroneously limited to a length of 21 characters. This issue was fixed.
Certain issues regarding the conversion of netmask notation types in Barracuda NG Admin were fixed.
Authentication options TACACS+ and NGF Local were erroneously not available for NG Control Center Admins. This issue was fixed.
The ***Open Configuration for...*** dialog in the Control Center Status map did not work as intended if logging in was carried out using a DNS name instead of an IP address. This issue was fixed.
It was erroneously possible to add duplicate entries to configuration lists. This issue was fixed.
Attempts to log in using an unresolvable hostname were generating a meaningless error message instead of pointing the user to the actual problem. This issue was fixed.
In firmware release versions 5.2.x, it was erroneously not possible to export a whole set of licenses to the clipboard or to use the ***Copy***, ***Merge*** and ***Replace*** buttons for more than one license concurrently. This issue was fixed.
On a Barracuda NG Control Center, it was erroneously not possible to check the checkboxes in the ***Name*** column within ***Control > Firmware Update*** if the dialog was displayed on the secondary monitor of the workstation. This issue was fixed.
Barracuda NG Admin 5.2.x crashed on Barracuda NG Control Center units if a file was dragged from the ***Files*** section within ***Control > Firmware Update*** to the main section above. This issue was fixed.
It was erroneously not possible to remove multiple connection objects or interface groups from a forwarding rule at once. As soon as more than one item was selected, the ***Delete*** button didn't have any effect anymore. This issue was fixed.
Copying and pasting access groups within ***Infrastructure Service > SNMP Service Settings*** caused the loss of ***View*** settings in the target node. This issue was fixed.

Barracuda NG Installer

Table 1–5 Barracuda NG Admin

Description
In rare cases, certain units were erroneously detected as XEN units. This issue was fixed.

Barracuda NG Network Access Client 2.0 SP6

Table 1–6 Barracuda NG Admin

Description
The `FWOFF` and `FWON` switches of the `rvpn` command line tool did erroneously not work in a shell window with admin rights. This issue was fixed.
The client erroneously crashed with a bluescreen if more than 16 different DNS servers were configured. This issue was fixed.
The PPP adapter was erroenously contained within the list of adapters in the Personal Firewall. This issue was fixed.
Multiple X.509 certificates found in the ***Local Computer*** certificate store did not precipitate proper error handling. This issue was fixed.
X.509 certificates extending their validity beyond the year 2038, which is the last valid year in unix time code, caused problems with the client as it could not read the expiration time value. This issue was fixed.
Under certain circumstances, the client's profile wizard crashed if the profile was using X-509 certificates. This issue was fixed.
Under certain circumstances, the client's profile wizard was not able to update stored settings as intended. Instead, it changed these settings to their default values. This issue was fixed.
Rekeying a key after the configured period of time did not work as intended. This issue was fixed.
The rekeymaxbytes default value did not have the intended effect. This issue was fixed.
It was erroneously not possible to configure values within the HKEY_CURRENT_USER registry hive on controlled clients. This issue was fixed.
Multi-monitor support lacked to work as intended regarding tray notification dialogs. This issue was fixed.
The client service (`phions.exe`) could erroneously crash when a VPN group name contained special characters. This issue was fixed.
X.509 handling was erroneously not possible when no crypto provider was available. This issue was fixed.

Barracuda NG Firewall

Table 1–7 Barracuda NG Firewall

Module	Description
Access Control Service	An issue with the Dutch keyboard layout causing the VPN applet to erroneously activate the German keyboard layout was fixed.
Authentication Service	The Authentication Service was erroneously not able to authenticate users to certain services if they were member of only the default domain user group. This issue was fixed.
Barracuda OS	Deactivated box services were erroneously displayed with red status indicators in ***Control > Processes***. This issue was fixed.
Barracuda OS	On legacy netfence edge units, the status LED erroneously kept flashing after an installation process was already finished. This issue was fixed.
Barracuda OS	Firewall rule names exceeding a length of 64 characters were breaking their respective log files, which was on Flash-based units occasionally resulting in the log service consuming all available system resources, eventually ending up in a system crash. This issue was fixed.
Barracuda OS	BIND was updated in order to fix a vulnerability. See also https://www.isc.org/software/bind/advisories/cve-2011-4313.

Table 1–7 Barracuda NG Firewall

Module	Description
Barracuda OS	The activation of standard hardware (SF) licenses did under certain circumstances fail, generating obfuscating and meaningless error messages. The problem appeared only on hardware units, not on virtual machines. This issue was fixed.
Control Center	Downloaded files were erroneously not restored on reinstalling the system. This issue was fixed.
Control Center	Activating SF single licenses erroneously failed on Barracuda NG Control Center units. This issue was fixed.
Firewall	On very rare occasions, a unit could freeze due to the usage of local redirect rules. This issue was fixed.
Firewall	The NG Firewall Ticketing System (ticketing management feature at the landing page) erroneously displayed a validity date that was one month back. This issue was fixed.
Firewall	In rare cases, units with 64-bit multi-core architecture could freeze due to a problem related to inbound IPv6 traffic. This issue was fixed.
Firewall	In rare cases, adding or deleting tickets in the ticketing system's landing page failed in saving changes to the database, throwing users back to the login page instead. Furthermore, trying to print a ticket using Internet Explorer 9 brought up the following error message: `Your browser is not supported. Please use a supported browser!` Such an attempt to print a ticket in Firefox would print the ticket as intended but would also subsequently redirect the user to an empty page. These issues were fixed.
Firewall	In firmware release version 5.2.2, MSCHAP authentication did in certain cases not work if the firewall's Intrusion Prevention System (IPS) feature was activated. This issue was fixed.
Firewall	Filling in an IP address and an interface name within ***IP / Ref i***n a Network Object while the Kernel Ruleset is set to ***yes*** prevented the respective firewall rule from working. This issue was fixed.
Firewall	Setting ***SynFloodProtection*** to ***Inbound*** and having a ***Redirect*** firewall rule cycling through two destination servers could cause a problem with destination server reachability in case one of the destination servers went down and came back to life later. It was not recognized as being reachable then. This issue was fixed.
Firewall	The landing page did not allow usage of the 'ß' character in user names. This issue was fixed.
Firewall	Synchronous pinging from one Windows system to another Windows system and vice versa through the Firewall was erroneously not possible. This issue was fixed.
Firewall	An issue regarding invalid TCP header checksum errors in local connections, mostly VPN TCP connections, with ***TCP Checksum Validation*** switched off in the general firewall configuration, was fixed.
Firewall	On Internet Explorer 9, the landing page did at a certain point not redirect users after the welcome screen as intended. Instead, it reloaded itself but with a missing background image. This issue was fixed.
HTTP Proxy	Setting the Safe Search option to Strict had no effect. This issue was fixed.
HTTP Proxy	The HTTP Proxy was under certain circumstances not able to start when no authentication text was configured. This issue was fixed.
Mail Gateway	In rare cases, HA synchronization of the Mail Gateway did not work as intended as email data was synced to the primary unit but at the same time not deleted from the secondary box. This would then cause a loss in performance and raise the latency of the email flow after a while, or it could even result in exceeding the maximum session limit. This issue was fixed.
Network	Configuring an IPv6 route with unnecessary, but valid leading zeros led to the route displayed as wild although the notation was valid and the route was working as intended. This issue was fixed.
Network	On models with WiFi, it was erroneously not possible to choose the ***ath2*** WiFi interface within the routing configuration. This issue was fixed.
Network	In rare cases, OSPF introduced routes were not introduced as intended, because, under certain circumstances, summary routes received from OSPF neighbors were not written into the routing table. This issue was fixed.

Table 1–7 Barracuda NG Firewall

Module	Description
Network	The ***TKIP*** encryption mode was erroneously configurable to work in ***WPA2*** security mode. The WiFi service refused to start up if this combination was configured. This issue was fixed.
Secure Web Proxy	The selection chosen in the ***Select Target Address*** list was erroneously not shown, This issue was fixed.
SNMP Service	The SNMP Service was erroneously not able to fetch certain operational values from an unit's internal sensors. This issue was fixed.
SNMP Service	The SNMP Service's configuration interface erroneously still displayed old OIDs in addition to the new ones after the configuration was changed and activated. This issue was fixed.
Virus Scanner	The Virus Scanner was in rare cases rejecting certain PDF files after erroneously classifying them as malware. This issue was fixed.
VPN Service	Activating packet compression could lead to the transport of some malformed packets. Although this was not a security risk, it could cause unwanted effects on the receiving side. This issue was fixed.
VPN Service	A problem with downwards compatibility was under certain circumstances causing Barracuda NG Network Access Clients older than 2.0 SP4 to disconnect by transmitting an incompatible ruleset. This issue was fixed.
VPN Service	Site-to-Site tunnels using GCM authentication were erroneously terminated due to authentication timing problems. This issue was fixed.
VPN Service	The user name was not correctly transmitted to the VPN server when using RADIUS as authentication method if the user name string was containing '\n' as the starting sequence for the user name part. This issue was fixed.
VPN Service	In rare cases, kernel memory limitations on 32-bit systems caused units to freeze due to a problem with the VPN packet stack. This issue was fixed.
VPN Service	WANOPT would under certain circumstances hang due to a race condition. This issue was fixed.

Supported Hardware

Table 2–8 Barracuda Networks Appliances Supported By Barracuda NG Firewall 5.2.3

Barracuda Networks Appliances Supported by Barracuda NG Firewall 5.2.3
Hardware Appliances: **Full Support:** F10, F15, F100, F101, F200, F201, F300, F301, C400, C610, F400, F600, F800, F900 **Beta Support:** F10 Rev.B, F100 Rev.B, F101 Rev.B, F200 Rev.B, F201 Rev.B, F300 Rev.B, F301 Rev.B
Virtual Appliances: VF25, VF50, VF100, VF250, VF500, VF1000, VF2000, VF4000, VF8000, VC400, VC610, VC820

Table 2–9 Legacy Appliances and Standard Hardware Supported By Barracuda NG Firewall 5.2.3

Legacy Appliances and Standard Hardware Supported by Barracuda NG Firewall 5.2.3
Legacy Hardware Appliances*: netfence edge Rev.B, sintegra XS Rev.B, sintegra S Rev.B, sintegra SR Rev.B, netfence S, netfence SR, netfence E, netfence XL, MR, M1, M3 Rev.A, M3 Rev.B, sintegra XS, sintegra S, sintegra S Rack, netfence edge Rev.A, netfence 140, netfence 240, netfence 240 Rack, netfence 421, netfence 431, netfence 780, netfence 850, S6 Rev.A, S6 Rev.B, S16, M50, L2000, industrial appliance, netfence L
Standard Hardware: This refers to hardware which is neither a Barracuda Networks nor a legacy phion appliance. Please follow the instructions given in the chapter **Updating Standard Hardware from 4.2.x to 5.2.3, page 58**.

* See the ***Barracuda NG Firewall 5.2 Migration Instructions*** for important information on restrictions appearing with certain legacy appliances on updating from firmware release versions below 5.0.

Determine Your Update Scenario

Caution

As soon as a unit has been updated to firmware version 5.2.3 and, subsequently, any new features were configured using Barracuda NG Admin 5.2.1 or 5.2.3, **no configuration changes must be made anymore using versions of Barracuda NG Admin prior to version 5.2**! Doing so could destroy the configuration.
Always use Barracuda NG Admin 5.2.3 together with Barracuda NG Firewall 5.2.3.

Note

Updating to Barracuda NG Firewall 5.2.3 is possible from firmware release version 5.0 and newer. Direct updating from release versions prior to 5.0 is not possible. Update to 5.0 first.

Note

To install Barracuda NG Control Center C400 or C610 appliances from the thumb drive, it is necessary to change the boot device order within the BIOS. Therefore you will need the unit's BIOS password. You can obtain that password through the Barracuda Networks Technical support.

Note

In case you are updating a HA synchronized unit to firmware release version 5.2.3 while not updating its secondary unit as well, or vice versa, so that the units run on different firmware versions, it may be necessary to re-synchronize the units after updating. To do so, click ***Firewall > Live > Show Proc***, select the process named ***Sync Handler*** and choose ***Kill Selected***. Session synchronization will automatically re-appear subsequently.

Note

In order to use Microsoft Exchange 2010 via SSL VPN after updating to Barracuda NG Firewall 5.2.3, it is necessary to perform ***Activate*** at least once within the ***SSL VPN*** settings in Barracuda NG Admin to correctly apply the update to the SSL VPN engine.

Note

See Supported Hardware, page 49 to determine whether your Barracuda hardware qualifies for a supported installation of or a supported update to Barracuda NG Firewall 5.2.3.

If you are going to update so-called "standard hardware" from a firmware version prior to 5.0, please follow the instructions given in ***Updating Standard Hardware from 4.2.x to 5.2.3***, page 58.

Updating requires at least 50 MB of free space on the `/boot/` partition.
However, if there is under firmware release versions 5.0.x or 5.2.x less space then 50 MB left, you may free up additional space by performing the following workaround.

If you need to perform the workaround on a huge number of managed units, you may execute it as a remote execution script on the Barracuda NG Control Center. Remote execution scripts are configurable under ***Control > Remote Execution***.

Note

By performing this workaround, ART will not be at your disposal during the updating process but will become available again once the updating process is finished.

- ***Within Barracuda NG Admin, open an SSH connection to the unit***
- ***Delete a certain file using the command*** `rm -f /boot/art/art.tar.gz`
- ***Go ahead to the updating process***

Before beginning the updating process, you should clarify which types of hardware and administrative configuration you have.
Barracuda NG Firewall 5.2.3 allows different administrative configurations. Please follow those update instructions applying to your configuration.

Table 2–10 Different Administrative Configurations

Administrative Configuration Type	Applicable Update Instructions
Unmanaged Unit or NG Control Center	If you want to update either **an unmanaged unit or an NG Control Center**, then proceed to ***Updating Unmanaged Units or NG Control Centers, page 53***.
NG Control Center Managed Unit	If you want to update **a unit that is managed by an NG Control Center**, then proceed to Updating NG Control Center Managed Units, page 56. f you also need to update **a cluster or a range of NG CC-managed units**, proceed subsequently to Updating Standard Hardware from 4.2.x to 5.2.3, page 58.
Unit or NG Control Center **combined with HA Unit**	If you want to update **a unit or an NG Control Center** (that is **combined with a High Availability (HA) unit**, then proceed to Updating HA-Synced Units or HA-Synced NG Control Centers, page 54. f you also need to update **a cluster or a range of NG CC-managed units**, see the **Barracuda NG Firewall 5.2 Migration Instructions** available for download at **http://barracuda.com/doc**.

Combining NG Control Center 5.2.x with 5.0.x and/or 4.2.x Units

The table below shows compatibility between the firmware's major versions.

Table 2–11 Firmware compatibility

Unit Version	Barracuda NG Control Center Version			
	phion netfence management centre 4.2.X	Barracuda NG Control Center 4.2.X	Barracuda NG Control Center 5.0.X	Barracuda NG Control Center 5.2.X
netfence 4.0.X	✓	-	✓	✓
netfence 4.2.X	✓	-	✓	✓
Barracuda NG Firewall 4.2.X	-	✓	✓*	✓*
Barracuda NG Firewall 5.0.X	✓**	✓**	✓	✓
Barracuda NG Firewall 5.2.X	-	-	✓**	✓

* Already existing units only; introduction of new units, especially new Barracuda appliances is not possible.

** Configuration sent from the Barracuda NG Control Center to the unit is automatically migrated on the unit. Newly introduced features of the respective release can't be configured. The managed unit migrates the configuration automatically by itself and sets initial default values for newly introduced configuration items.

Solving Update and Installation Failures

If a unit does not boot into normal operation mode after update or installation, certain BIOS settings might be misconfigured.

Note

In order to access the BIOS, it may be necessary to obtain your unit's BIOS password through the Barracuda Networks Technical Support first.

Reset the BIOS configuration by performing the following steps:

- ***Establish a serial console connection to the unit (19200 bit/s).***
- ***Switch the appliance on and hold the Del key during the boot-up RAM test. Wait until the BIOS screen appears.***
- ***If the BIOS screen does not appear, hold ALT and simultaneously press 0 on the numeric keyboard. Then, release 0 again while still holding ALT and, again simultaneously, press 9 on the numeric keypad, followed by releasing 9 and finally also releasing ALT. The BIOS screen should appear.***
- ***Within the BIOS menu, select and execute Set to optimal defaults.***
- ***Save the new settings, exit the BIOS and reboot the appliance.***

Updating Unmanaged Units or NG Control Centers

Updating Units or NG Control Centers using SSH

Best Practice

For speed reasons, Barracuda Networks recommends using this method of updating for all appliances in general, especially for those based on a flash drive or slower hardware.

Step 1: Copy

Before copying the package onto the unit as described below, make sure that there is no old minor release or patch package lurking within the `/var/phion/packages/` directory. The directory must not contain any files.

Although the `/var/phion/packages/` directory must be empty, it still contains the subdirectories: `kl, os, ph, sa, tgz`. These don't affect the updating process. Furthermore, there must not be a whitespace character within path or file name of the package.

- ***Copy the update package onto your firewall system into the*** `/var/phion/packages/` ***directory of the respective unit.***

To get the file onto the unit, you may use the ***Send File*** button within the built-in SSH client of Barracuda NG Admin. Don't forget to change the directory first using `cd /var/phion/packages/`.

Step 2: Update

Start the update sequence by executing `phionUpdate` from the shell.

No more interaction is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning

Do not interrupt the update procedure. During update, the unit boots several times and due to this, the connection will be terminated. Whether the update process has been successfully finished is confirmed by output on the console, log messages, and firmware version and status displayed within ***Control > Licenses.***

Updating HA-Synced Units or HA-Synced NG Control Centers

In the instructions below, the term "primary unit" refers to the unit used for regular operation, while "HA unit" refers to the secondary unit used as a failover system.

Caution

For Firewall and Configuration HA synchronizing with one of the units running 5.2.x, the other unit in the HA partnership must run at least firmware release version 5.0. HA synchronizing between a 5.2.x unit and a 4.x unit is not possible.

Barracuda Networks strongly recommends to follow the procedure for updating HA systems exactly as described below in order to minimize any operational drop outs.

Step 1: Prepare the HA Unit

- ***Log-in to the HA unit using Barracuda NG Admin.***
- ***Block the (standby) server on the HA unit within Control > Server.***

Step 2: Update the HA Unit

- ***Update the HA unit using SSH as delineated in Updating Units or NG Control Centers using SSH, page 53.***

No more interaction with the HA unit is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning

Do not interrupt the update procedure. During update, the unit boots several times and due to this, the connection will be terminated. Indicators that the update process has been finished are the following output on the console: `Barracuda NG Firewall release 5.2.3-xxx`, or the operativeness of logging in again using SSH or Barracuda NG Admin.

Step 3: Switch Servers to the HA Unit and Prepare the Primary Unit

- ***Log-in to the primary unit using Barracuda NG Admin.***

Proceed after having assured that the HA unit is fully functional.

- ***Unblock the (standby) servers on the HA unit by clicking Stop Server within Control > Servers.***
- ***Log-in to the primary unit using Barracuda NG Admin.***
- ***Switch all servers from the primary to the HA unit and verify for correct operability. Therefore, Block all Servers on the primary unit.***

You may leave the primary unit in standby mode until correct operability of the HA unit has been verified. Click *Stop Server* on the primary unit in order to achieve this. If functional errors occur on the HA unit, you may switch servers back to the primary unit.

Step 4: Update the Primary Unit

- ***Update the primary unit using SSH as delineated above in Updating Units or NG Control Centers using SSH, page 53.***

No more interaction with the primary unit is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning

Do not interrupt the update procedure. During update, the unit boots several times and due to this, the connection will be terminated. Whether the update process has been successfully finished is confirmed by output on the console, log messages, and firmware version and status displayed within ***Control > Licenses.***

Step 5: Switch Servers Back to the Primary Unit

- ***Log-in to the respective primary unit using Barracuda NG Admin.***

Proceed after having assured that the primary unit is fully functional.

- ***Re-enable all servers on the primary unit by clicking Stop Server (Control > Server) on each.***
- ***Log-in to the HA unit using Barracuda NG Admin.***
- ***Block all the servers on the HA unit by clicking Block Server (Control > Server).***

Proceed after having assured that the primary unit is fully functional.

- ***Set all the servers on the HA unit back to standby by clicking Stop Server (Control > Server).***

The update process is finished.

Updating NG Control Center Managed Units

To make use of the multi-release capabilities of Barracuda NG Control Center, all units within one cluster must run under the same software major release version. Migration of the NG CC configuration is only available for all units, servers and services of a cluster simultaneously.

Step 1: Import the Update Package into the NG Control Center

- ***Log-in to the Barracuda NG Control Center using Barracuda NG Admin.***
- ***Navigate to** Control > Firmware Update **and click** Import...*
- ***Select the update package within the file browser.***

Step 2: Select Units to Update and Send them the Update

- ***Choose the desired** Range**,** Cluster **or** Box**.***
- ***Select the previously copied update within the** Files **list.***
- ***Click** Create Task...*
- ***Choose** Immediate Execution **from the** Scheduling **drop-down menu and click** OK**.***

Step 3: Execute the Copied Update

- ***Navigate to** Control > Update Tasks.*
- ***Verify if the update package was successfully copied, which is indicated by a green icon within the** Σ **column.***
- ***Right-click the desired unit and select** Perform Update **followed by choosing** Immediate Execution **from the** Scheduling **drop-down menu and clicking** OK.*

No more interaction with the unit is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Note

Take a look into the box log file at ***Box > Logs >*** `Box\Release\update` after the update process has been finished. In case of a not succeeded update please consult `Box\Release\update_hotfix` for a detailed log.

Updating Standard Hardware from 4.2.x to 5.2.3

General

Due to a kernel version change between 4.2.x and 5.2.3 (linux kernel 2.4 was changed to linux kernel 2.6), the enumeration of NICs may on some hardware sort the ethX devices in a different order, resulting in a loss of management access.

Therefore, a procedure has now been implemented to rename the interfaces after upgrading to 5.2.3 to remain identical with the 4.2.x interface names. This is done by creating an interface mapping table using the eth device's MAC addresses as identifiers.

The following procedure **must be performed on every single unit seperately** due to the fact the MAC addresses are different per unit and so will be the mapping table.

If you find out later that your server is not affected by the resorting issue, then you may delete the mapping configuration subsequently. The network activation log will then contain the following message:

```
No difference found between configured and detected MAC to interface mapping
```

- ***Update is possible on standalone as well as on NG CC-managed units from firmware 4.2.0 onwards to major release version 5.0. No direct updating to 5.2.x is possible!***
- ***Updates from a base release in the range from 4.2.0 to 4.2.14 requires a hotfix to be installed. 4.2.15 to 4.2.18 include the functionality, therefore no hotfix is required.***
- ***It is recommended to evaluate the process on a system with physical access or in a lab environment in case the upgrade fails.***
- ***The procedure is compatible with user defined interface mappings. If a user defined interface mapping is found, it will be applied after the MAC-to-eth mapping procedure.***
- ***If you add additional NICs after upgrading to 5.0, the mapping may fail. Therefore, do not use MAC mapping in this case any longer but switch to user defined interface mapping. The problem may occur if linux detects the new NICs before it detects the old ones.***

Updating Procedure

Step 1: Prepare the Standard Hardware For the Update

- ***If the unit runs on firmware 4.2.14 or below, you must install the hotfix*** `boxnet_mac2ifmapping-386-4.2.14`***.***

Step 2: Generate the Mapping Data

- ***Log into the unit via ssh as root and issue the following command:***
  `CreateMACMapping`
  Running this program multiple times will do no harm.
- ***Copy the output lines of the program beginning with*** `CM` ***and those beginning with*** `CI` ***to the clipboard.***

Step 3: Apply the Mapping Data

- ***On standalone units, open the Box Network Configuration within Barracuda NG Admin.***
  On NG CC-managed units, open the Box Network Configuration within Barracuda NG Admin on the respective Barracuda NG Control Center.
- ***Paste the content of the clipboard to Network > Interfaces > MAC Mapping (only visible in Advanced configuration mode).***
- ***Set Use Assignment to yes.***
- ***Click Send Changes followed by Activate.***

Step 4: Proceed to the Update

- ***Upgrade the unit following the 5.0 upgrade procedure as described in the separately available Barracuda NG Firewall 5.0 Migration Instructions. Please download this document from*** **http://barracuda.com/doc.**
- ***Subsequently, you may update from 5.0 to 5.2.3 following the procedures as described in Determine Your Update Scenario, page 50.***

When the update process is finished, please verify if all interfaces are correctly mapped.

Note

In case the linux kernel 2.4 assigned the interfaces in the same order as the linux kernel 2.6 did, the following message will be generated into the 5.0 box network activation log:

```
No difference found between configured and detected MAC to interface mapping
```

In this case you may disable MAC mapping. This will make the configuration hardware-independent, providing you with more flexibility in case hardware will be changed somewhen in the future.

Note

Further advice about updating standard hardware is available through the Barracuda Networks support.

Barracuda Networks Technical Documentation

RECLAIM YOUR NETWORK™